Учреждение образования
«Белорусский государственный университет культуры и искусств»
Факультет информационно-документных коммуникаций
Кафедра информационно-аналитической деятельности

СОГЛАСОВАНО
Заведующий кафедрой
_____Н.А.Яцевич
22.09.2022 г.

СОГЛАСОВАНО
Декан факультета
_____Ю.Н.Галковская
23.09.2022 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Информационная безопасность библиотечно-информационных систем

для специальности второй ступени высшего образования (магистратура)
1-23 80 01 – Библиотечно-информационная деятельность.
Профилизация: Теория и методика научно-исследовательской и аналитической деятельности

Составитель: Н.А. Яцевич,
кандидат педагогических наук,
доцент

Рассмотрено и утверждено
на заседании Совета университета
27 сентября 2022 г.,
протокол № 1.

Минск 2022

Составитель:

Яцевич Николай Александрович, заведующий кафедрой информационно-аналитической деятельности учреждения образования «Белорусский государственный университет культуры и искусств», кандидат педагогических наук, доцент

Рецензенты:

Григянец Ромуальд Брониславович, заведущий лабораторией Объединенного института проблем информатики Национальной академии наук Беларуси, кандидат технических наук, доцент

Касап Вера Александровна, профессор кафедры информационных ресурсов и коммуникаций учреждения образования «Белорусский государственный университет культуры и искусств», кандидат педагогических наук, доцент

Рассмотрен и рекомендован к утверждению:

Кафедрой
информационно-аналитической деятельности
(протокол от 31.08.2022, № 1.);

Ученым советом Центральной научной библиотеки им. Якуба Коласа Национальной академии наук Беларуси

(протокол от 27.05.2022, № 3)

Советом факультета информационно-документных коммуникаций учреждения образования «Белорусский государственный университет культуры и искусств»

(протокол от 20.09.2022, № 1)

СОДЕРЖАНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная дисциплина «Информационная безопасность библиотечно-информационных систем» в учебном плане магистерской подготовки по специальности 1-23 80 01 Библиотечно-информационная деятельность входит в государственный компонент (*модуль «Методология и методика научных исследований”).*

Целью учебной дисциплины является овладение магистрантами знаниями и умениями управления информационной безопасностью в библиотеке в целом, ее библиотечно-информационных технологиях, а также предотвращения потенциальных информационных угроз.

Содержание учебной дисциплины, а также перечень компетенций, которыми должны владеть выпускники магистратуры представлены в учебной программе (раздел 5.1).

Учебно-методический комплекс (УМК) по учебной дисциплине «Информационная безопасность библиотечно-информационных систем» представляет собой систему дидактических средств обучения. Он является структурно-логической моделью процесса формирования перечисленных в учебной программе профессиональных компетенций магистра в сфере информационной безопасности библиотеки.

Цель УМК по учебной дисциплине «Информационная безопасность библиотечно-информационных систем» заключается в систематизации учебно-методических материалов, необходимых для изучения теории и практики информационной безопасности библиотек и защиты их информационных ресурсов.

Задачи УМК:

- систематизация содержания учебной дисциплины «Информационная безопасность библиотечно-информационных систем»;
- упорядочение процесса изучения учебной дисциплины;
- обеспечение организации самостоятельной учебной работы и контроля знаний студентов;
- оказание магистрантам методической помощи в усвоении учебного материала;
- оказание преподавателям методической помощи, необходимой и достаточной для качественного преподавания данной учебной дисциплины.

Особенности структурирования УМК и подачи материала в нем определяются: изданной в 2021 году учебной программой по данной учебной дисциплине; требованиями к компетенциям, которыми должен владеть магистрант в результате изучения учебной дисциплины, «Положением об

учебно-методическом комплексе на уровне высшего образования», утвержденным Постановлением Министерства образования Республики Беларусь 8.11.2022, № 427.

Примерное распределение учебных часов по видам занятий в соответствии с рабочим учебным планом для очной и заочной форм получения высшего образования представлено в разделах 5.2 и 5.3 данного УМК. Рекомендуемая форма контроля занятий студентов – зачет.

2. ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ
2.1. Конспект лекций

Тема 1. Информационная безопасность как интегральная научно-практическая проблема

Информационная безопасность является сложным понятием, которое можно трактовать в «широком» и «узком» значении, что зависит от многих факторов: области деятельности, объектов и субъектов защиты, видов информационных угроз, методов и средств защиты информации и т.д. Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл.

В «Концепции информационной безопасности Республики Беларусь» (2019 г.) она определяется универсально, как «состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере».

Несомненно, что информационная безопасность является областью научной и практической (профессиональной) деятельности. В научном плане существует множество подходов к определению этого понятия. Однако все они, как правило, сводятся к тому, что в основе информационной безопасности лежит деятельность по *защите информации,* обеспечению её *конфиденциальности, целостности* и *доступности*, что это – практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения или уничтожения информации.

Защита информации согласно Закону Республики Беларусь «Об информации, информатизации и защите информации» (2008 г.), это – «комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации».

Таким образом, *информационная безопасность* базируется на трех ключевых категориях: конфиденциальность, целостность и доступность (КЦД) информации. В этом заключается универсальность данного понятия. Оно применяется вне зависимости от формы (носителя), которые может принимать информация (данные) – бумажная, электронная, устная. Основная задача информационной безопасности – сбалансированная защита конфиденциальности, целостности и доступности информации. Это достигается в основном с помощью многоэтапного процесса управления рисками в информационной сфере, в том числе, в библиотечно-информационной деятельности.

Триада КЦД была определена еще в 1975 году в статье американских ученых в области компьютерных наук Джерри Зальцера и Майкла Шредера «Защита информации в компьютерных системах». Они предложили классифицировать нарушения безопасности на три основных категории: неавторизованное раскрытие информации (unauthorized information release), неавторизованное изменение информации (unauthorized information modification) и неавторизованный отказ в доступе (unauthorized denial of use) к информации. В 1998 году Донн Б. Паркер дополнил классическую триаду КЦД ещё тремя аспектами: *владение или контроль*, *аутентичность* и *полезность*.

Организация экономического сотрудничества и развития (ОЭСР), (организация развитых стран, признающих принципы представительной демократии и свободной рыночной экономики) представила в 1992 году девять принципов информационной безопасности: *осведомленность, ответственность, противодействие, этика, демократия, оценка риска, разработка и внедрение безопасности, управление безопасностью, пересмотр.*

Существуют и другие модели информационной безопасности, например: американского Национального института стандартов и технологий, который сформулировал восемь принципов; министерства обороны США (три основополагающих принципа – *«подверженность системы риску», «доступность уязвимости», «способность эксплуатировать уязвимость»*); Международной федерации по стандартизации (ISO), которая рекомендует устанавливать взаимосвязи между информационной безопасностью и неприкосновенностью частной жизни (в ее стандарты уже включены дополнительные принципы – *подлинность, подотчетность, невозможность отказа*, *достоверность)* и другие.

Однако, классическая триада КЦД по-прежнему остаётся наиболее признанной и распространённой в международном профессиональном сообществе. Она зафиксирована в национальных и международных стандартах, законодательных и нормативно-правовых документах, вошла в основные образовательные и сертификационные программы по информационной безопасности.

Государственный стандарт Республики Беларусь СТБ 34.101.30-2007 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация» определяет КЦД следующим образом:

− *конфиденциальность* информации – свойство информации, определяющее необходимую степень ее защиты от несанкционированного

доступа и от использования ее субъектами, не имеющими соответствующих полномочий;

− *целостность* информации – свойство информации сохранять свое информационное содержание и однозначность интерпретации в условиях случайных и/или преднамеренных воздействий;

− *доступность* информации – свойство информации быть доступной за приемлемое время по запросу со стороны санкционированного субъекта.

Таким образом, к настоящему времени категории КЦД (CIA) стандартизировались и имеют следующие значения:

1. *Конфиденциальность (confidentiality)* – свойство информации быть недоступной или закрытой от несанкционированного доступа. Конфиденциальность информации понимается как обеспечение доступа к ней лиц, имеющих на это права с наименьшими привилегиями, исходя из принципа минимальной необходимой осведомлённости. Авторизованное лицо должно иметь доступ только к той информации, которая ему необходима для исполнения своих должностных обязанностей. При этом происходит классификация информации по степени доступности: строго конфиденциальная, предназначенная для внутреннего использования, предназначенная публичного использования. Самым типичным способом обеспечения конфиденциальности является шифрование информации.

2. *Целостность (integrity)* – свойство информации, заключающееся в неизменности (аутентичности), правильности и полноте данных в процессе хранения, передачи и использования, их защищенность. Информация, хранящаяся в базах данных, файлах, передаваемая по компьютерным сетям должна быть достоверной. Она должна быть защищена от изменений, искажений в процессе обработки, хранения, передачи и использования. Целостности информации угрожают: компьютерные вирусы, логические бомбы, ошибки программирования, вредоносные изменения программного кода; подмена данных; неавторизованный доступ; технические сбои; человеческие ошибки по оплошности или низкой профессиональной подготовке; случайное удаление файлов; ввод ошибочных значений, изменение настроек, выполнение некорректных команд и т.п. Для защиты целостности информации используется множество необходимых способов. Типичным примером таких мер является ограничение круга лиц, которые не имеют права на изменение данных. При этом, важно соблюдать принцип разграничения полномочий. Все действия по изменению информации должны фиксироваться и протоколироваться.

3. *Доступность (availability)* – возможность беспрепятственного получения информации и её использования субъектами, имеющими права доступа на ее чтение, копирование, изменение, уничтожение. Информация

должна быть доступна авторизованным лицам и тогда, когда это необходимо. На доступность информационных систем влияют отказы в обслуживании (DoS-атаки), программы-вымогатели, саботаж; человеческие ошибки; отказы в обслуживании; случайное удаление файлов или записей в базах данных и т.п, а также природные катаклизмы.

Информационная безопасность как система имеет следующие основные составляющие:

− научную;

− законодательную, нормативно-правовую базу;

− организационную (подразделения), обеспечивающие безопасность;

− способы и средства обеспечения информационной безопасности;

− информационно-психологическую составляющую;

− политику информационной безопасности (совокупность норм, правил, запретов и практических рекомендаций).

Все перечисленное в полной мере относится к библиотекам и их информационным системам как объектам информационной безопасности. Эти составляющие будут рассмотрены в настоящей учебной дисциплине.

На уровне государств существуют концептуальные документы, которые трактуют сущность информационной безопасности исходя из их национальных интересов: концепции, доктрины, акты, «радужные книги» (США) и т.п.

Как уже отмечалось, в Республике Беларусь – это «Концепция информационной безопасности Республики Беларусь», принятая Советом безопасности Республики Беларусь в 2019 году. Концепции основывается на Конституции Республики Беларусь, законодательстве Республики Беларусь в областях национальной безопасности, информатизации, развития цифровой экономики, информационного общества, науки и технологий, защиты интеллектуальной собственности, иных актах законодательства.

Концепция состоит из семи разделов:

1) общие положения (актуальность информационной безопасности, ее предмет, цель, задачи; основные понятия и определения);

2) состояние и развитие информационной сферы Республики Беларусь (гуманитарные и технологические аспекты);

3) государственная политика обеспечения информационной безопасности (цели, направления; информационный суверенитет и нейтралитет; реагирование на риски, вызовы и угрозы в информационной сфере;

4) безопасность информационного пространства как одного из важнейших условий развития государства (меры и основные направления

обеспечения информационной безопасности; сохранение традиционных устоев и ценностей, безопасность массовой информации);

5) обеспечение безопасности информационной инфраструктуры (меры и основные направления; безопасность национального сегмента интернет, киберустойчивость государственных информационных систем, противодействие киберпреступности);

6) обеспечение безопасности информационных ресурсов (основные направления, защита государственной и служебной тайны, защита персональных данных);

7) механизмы реализации концепции (подготовка нормативно-правовых актов, государственно-частное партнерство в сфере информационной безопасности, участие в обеспечении международной информационной безопасности).

В «Концепции информационной безопасности Республики Беларусь» отмечается, что основополагающим национальным интересом страны в информационной сфере с точки зрения гуманитарного аспекта является реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации, свободу мнений, убеждений и их свободного выражения, а также права на тайну личной жизни.

Тема 2. Библиотека как объект информационной безопасности

Библиотека как объект информационной безопасности представляет собой сложную организационно-функциональную систему, призванную обеспечить защиту имеющейся в ней информации и информационных ресурсов, зафиксированных на различных материальных носителях. В качестве *объекта защиты* информации может выступать сама информация или носитель информации, которые необходимо защищать в соответствии с целями защиты.

Защищаемая информация является предметом собственности и подлежит защите согласно требованиям правовых документов или требованиями, установленными собственником информации. Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо. В качестве *носителя защищаемой информации* может выступать физическое лицо или материальный объект, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин. В библиотеках создается *защищаемая информационная*

система, предназначенная для обработки информации с требуемым уровнем ее защищенности.

Объекты информационной безопасности.

Основные защищаемые объекты (информационные активы) информационной безопасности (ИБ) в библиотеке можно *условно* разделить на две основные группы: *материальные и нематериальные*.

К *материальным* объектам ИБ относят:

– охраняемая территория;

– здание библиотеки (помещения);

– библиотечный фонд;

– специальное оборудование (устройства для чтения микрофильмов, микрофиш и др.);

– сервера, компьютеры;

– периферийное оборудование, подключаемое к компьютеру (сканеры, принтеры, ксероксы, модемы);

– сетевые устройства (коммутаторы, концентраторы, маршрутизаторы, сетевые адаптеры, межсетевые экраны и другие);

– линии связи (кабель);

– носители данных (оптические диски, флеш-память).

К *нематериальным объектам* ИБ библиотеки относятся:

– электронные информационные ресурсы (электронный каталог, базы данных) свободного доступа, информационные ресурсы с ограниченным доступом, информационные ресурсы, защищенные авторским правом и лицензионными соглашениями;

– программное обеспечение для функционирования АБИС библиотеки (системное программное обеспечение – операционные системы), прикладное программное обеспечение, вспомогательное программное обеспечение (утилиты);

– веб-сайт библиотеки (информационные ресурсы сайта);

– информационные сервисы (виртуальные справочные службы, электронный читальный зал, электронная доставка документов и другие);

– система электронного документооборота библиотеки;

– права граждан, учреждений и организаций на доступ к информации и возможность получить ее в рамках закона;

– авторское право на информацию и информационные ресурсы;

– персональные данные пользователей и сотрудников;

– электронная платежная система;

– финансовое состояние библиотеки и другие.

Каждый объект не застрахован от уязвимостей, угроз и рисков информационной безопасности и предполагает особую систему мер защиты,

о которых речь пойдет ниже. Обеспечение информационной безопасности в каждом случае должно базироваться на системном подходе, учитывающем специфику объекта.

Согласно СТБ 34.101.30-2007 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация» в основу классификации объектов безопасности положены следующие принципы:

– *идентичности* по степени конфиденциальности обрабатываемой на них информации;

– *эквивалентности* (подобия) объектов по организации вычислительного процесса.

В СТБ устанавливаются следующие подклассы объектов защиты в зависимости от *степени конфиденциальности обрабатываемой информации*:

– подкласс 1 – совокупность объектов, на которых обрабатывается информация, содержащая сведения, отнесенные в установленном порядке к государственным секретам;

– подкласс 2 – совокупность объектов, на которых обрабатывается информация, содержащая сведения, отнесенные в установленном порядке к служебной информации ограниченного распространения, а также иная информация, охраняемая в соответствии с законодательством Республики Беларусь;

– подкласс 3 – совокупность объектов, на которых обрабатывается открытая информация.

Очевидно, что применительно к библиотекам в отношении ее объектов защиты в зависимости от степени обрабатываемой информации используются подклассы 2 – 3, так как информационные ресурсы библиотек (за исключением специализированных) не содержат информацию, которая отнесена к государственным секретам.

В зависимости от *организации вычислительного процесса* выделяется:

– подкласс А – совокупность объектов информатизации, технические средства которых размещены в пределах одной контролируемой зоны и обработка защищаемой информации осуществляется в пределах области действия комплекса средств безопасности объекта (КСБО). В библиотеках это автономный компьютер или группа компьютеров, размещенных в одном помещении; локальная сеть библиотеки; АБИС библиотеки, автоматизированные рабочие места библиотечных работников и др.;

– подкласс Б – совокупность объектов защиты, технические средства которых размещены в нескольких контролируемых зонах, объединенных открытыми или защищенными каналами передачи данных, и обработка информации осуществляется в пределах области действия КСБО. В этот

подкласс включается корпоративная сеть библиотеки и все ее подсистемы, объединенные между собой защищенными каналами передачи данных.

– подкласс В – совокупность объектов, технические средства которых размещены в одной контролируемой зоне и обработка защищаемой информации осуществляется в пределах области действия КСБО, но один или несколько из совокупности объектов имеют каналы обмена информацией, выходящие за пределы контролируемой зоны. В этот подкласс входят: локальная компьютерная сеть библиотеки, отдельный компьютер, подключенный к интернет. Эти объекты обрабатывают защищаемую информацию без ее передачи другим, внешним объектам.

Субъекты информационной безопасности.

В качестве субъектов информационной безопасности библиотеки выступают *персонал библиотеки* и *пользователи библиотеки.* Цель – защита субъектов информационных отношений от нанесения им материального, морального или иного ущерба путем воздействия на информацию и/или средства ее обработки и передачи.

Субъекты информационной безопасности заинтересованы в: своевременном оперативном доступе к необходимой информации; конфиденциальности информации; достоверности информации; защите от дезинформации; защите авторских прав; защите от незаконного тиражирования информации; контроле и управлении процессами обработки и передачи информации;

Субъекты информационной безопасности несут ответственность за:

− достоверность и полноту представляемой информации, генерированной самой библиотекой или полученной из внешних информационных систем;

− нарушение порядка распространения и (или) предоставления общедоступной информации и информации, представление которой ограничено в соответствии с законодательными актами;

− неправомерный доступ, уничтожение, изменение, использование и распространение информации;

− непринятие соответствующих мер по защите информации.

Угрозы, уязвимости и риски информационной безопасности.

Угрозы объектам информационной безопасности в библиотеке – это действия или события, которые могут привести к искажению, разрушению, уничтожению информации, программно-аппаратных средств, а также к неразрешенному использованию или блокированию правомерного доступа к ее информационным ресурсам. Угроза информационной безопасности библиотеке в общем смысле понимается как совокупность условий и

факторов, создающих опасность нанесения ей ущерба в чьих-то злонамеренных целях.

В качестве *источника угрозы* информационной безопасности может выступать субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной ее возникновения. Результатом реализации угрозы могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней. Видом описательного представления свойств или характеристик угроз информационной безопасности в библиотеке может быть специальный нормативный документ.

Существуют различные подходы (основания деления) к классификации угроз информационной безопасности. Признаки этих делений часто взаимно пересекаются. Опираясь на нормативно-технические документы, угрозы информационной безопасности библиотеки можно *классифицировать* по следующим признакам:

1. *По аспектам информационной безопасности*, на которые направлены угрозы:

– *угрозы конфиденциальности,* которые заключаются в неправомерном доступе к информационным ресурсам библиотеки. Информация становится известной тому, кто не имеет полномочий на ее получение. Такие угрозы возникают в основном в следствие «человеческого фактора», а также сбоев в работе программно-аппаратных средств компьютерной системы библиотеки;

– *угрозы целостности* данных, их неправомерное изменение, модификация информации, находящейся в базах данных библиотеки. Эти угрозы могут быть вызваны непрофессиональными или умышленными действиями персонала библиотеки и ее пользователями, выходом из строя АБИС библиотеки, ее программно-аппаратных средств;

– у*грозы доступности* – осуществление действий, блокирующих или затрудняющих доступ к АБИС и ее ресурсам, как внутри библиотеки, так и в удаленном доступе;

2. *По местонахождению источников угроз*:

– *внутренние* (источники угроз располагаются внутри самой библиотеки, ее информационно-коммуникационной инфраструктуры);

– *внешние* (источники угроз находятся вне библиотеки).

3. *По масштабам наносимого ущерба*:

– о*бщие* (нанесение ущерба библиотеке в целом, связанного в первую очередь с природными и катастрофными явлениями);

– *локальные* (причинение вреда отдельным информационным активам библиотеки, например, ее фонду);

– *частные* (причинение вреда отдельным частям элементов библиотеки, например, электронному каталогу).

4. *По степени воздействия* на информационно-коммуникационную систему библиотеки:

– *пассивные* (структура и содержание системы не изменяются);

– а*ктивные* (структура и содержание системы подвергается изменениям).

5. *По природе возникновения*:

– *естественные (объективные),* вызванные воздействием на библиотеку природных явлений, не зависящих от воли человека;

– *искусственные (субъективные)*, вызванные воздействием на информационную сферу пользователя и персонала библиотеки. Среди искусственных угроз можно выделить: *непреднамеренные (случайные)* (ошибки программного обеспечения, персонала, сбои в работе АБИС, отказы компьютерной техники и коммуникационного оборудования); *преднамеренные (умышленные)*, которые обусловлены действиями субъектов информационной безопасности библиотеки (неправомерный доступ к информационным ресурсам, использование и распространение программ неправомерного доступа, вирусных программ и т. д.). Преднамеренные угрозы могут стать причиной правонарушений и преступлений.

6. *По источникам угроз:*

– *антропогенные (субъектные)* – действия субъектов, которые могут привести к нарушению информационной безопасности библиотеки. Они бывают как умышленные, так и случайные, как внутренние, так и внешние. В библиотеке необходимо прогнозировать такие действия и принимать адекватные меры воздействия;

– *программно-технические,* которые являются менее прогнозируемыми, напрямую зависят от технических средств, используемых в библиотеке, их уязвимостей, и поэтому требуют особого внимания. Данные источники угроз информационной безопасности также могут быть как внутренними, так и внешними;

– *стихийные источники* – обстоятельства, вызванные стихийными бедствиями или другими обстоятельствами, имеющие объективный характер, которые невозможно предусмотреть или предотвратить, или возможно предусмотреть, но невозможно предотвратить, трудно прогнозировать. Стихийные источники (природные катаклизмы), как правило, являются внешними по отношению к библиотеке.

Уязвимость информационной безопасности библиотеки понимается как недостаток или слабое место (брешь) в названных выше ее объектах безопасности, средствах контроля и управления, которые могут быть

использованы злоумышленниками. Используя недостатки в системе ИБ, можно намеренно нарушить её целостность, вызвать неправильную работу всех систем. Применительно к информационно-коммуникационной системе библиотеки – это потенциальная возможность реализации угроз безопасности обрабатываемой в ней информации.

Считается, что сами по себе уязвимости информационной безопасности не опасны, но они открывают возможности для осуществления угроз ИБ. К наиболее распространенным причинам возникновения уязвимостей в библиотеках, как правило, относят: ошибки при проектировании и использовании АБИС; несанкционированное внедрение и использование нелицензионного программного обеспечения; внедрение вредоносного программного обеспечения; человеческий фактор и другие.

Уязвимость без наличия угрозы, возможно, и не требует контроля, но она должна быть найдена и необходим ее мониторинг на предмет изменений. Напротив, угроза без сопутствующих ей уязвимостей, возможно, не приведёт к риску. Уязвимости могут быть идентифицированы в следующих элементах библиотеки: персонале, организации работы, процедурах осуществления библиотечно-информационных процессов, конфигурации АБИС, аппаратных средствах, программном обеспечении, оборудовании, связи и т.д.

Существует большое число классификаций уязвимостей информационной безопасности. Их можно подразделить на *объективные* (обусловленные особенностями технических характеристик программно-аппаратных средств обеспечения), *субъективные* (возникшие вследствие ошибок в программировании, действиях пользователей библиотеки, системных администраторов) и *случайные* (возникшие вследствие непредвиденных обстоятельств).

Также можно выделить такие виды уязвимостей, как: *технологические* или *архитектурные*, выражающиеся в недостатках при проектировании системы; *организационные*, выражающиеся в отсутствии в библиотеке регламентированных процедур и системы обеспечения информационной безопасности; *эксплуатационные,* связанные с недостатками в эксплуатации АБИС и всей информационно-коммуникационной структуры библиотеки.

Некоторые уязвимости появляются из-за недостаточной проверки данных, вводимых пользователем в систему, из-за ненадежности паролей и другого. Необходимо постоянно обеспечивать защищённость и целостность коммуникационной системы библиотеки, постоянно следить за ней, устанавливать обновления, использовать инструменты, которые помогают противодействовать возможным атакам на ее основные объекты информационной безопасности.

В таблице 3 представлены примеры уязвимостей и примеры угроз на отдельные объекты ИБ библиотеки. Таблица составлена на основании международного стандарта ISO/IEC 27005:2011 «Информационная технология. Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности».

Риск – это вероятностная оценка величины возможного ущерба, который может понести библиотека при отсутствии в ней комплексной системы информационной безопасности. Информационная безопасность ассоциируется с потенциалом угроз, которые используют уязвимости объектов информационной безопасности и таким образом наносят ущерб библиотеке. Если уязвимость соответствует угрозе, то существует риск.

Таблица 1. Примеры уязвимости объектов информационной безопасности библиотеки.

Объект ИБ	Примеры уязвимости	Примеры угроз
Аппаратные средства (компьютеры, периферийные устройства, сетевое оборудование и др.)	Недостаточное обслуживание/ дефектная установка и подключение	Нарушение ремонтопригодности системы Разрушение оборудования или носителей информации
	Изъяны в схемах электрических соединений	
	Несоблюдение санитарно-гигиенических норм (влажность, пыль, загрязнение и др.)	Пыль, коррозия, обледенение
	Чувствительность к электромагнитной радиации	Электромагнитная радиация, нарушение здоровья человека
	Изъяны контроля набора комплектующих (конфигурации)	Ошибка в использовании
	Восприимчивость к изменениям напряжения	Потеря источника питания
	Восприимчивость к температурным изменениям	Метеорологическое явление
	Незащищенное хранение	Кража оборудования или документов
	Неконтролируемое копирование	Кража носителей или документов
	Отсутствие или недостаточное тестирование	Злоупотребление правами
	Известные недостатки в	Злоупотребление

Программное обеспечение	программном обеспечении	правами
	Нет «выхода из системы» при оставлении рабочей станции	Злоупотребление правами
	Передача или многократное использование носителей данных без надлежащего стирания	Злоупотребление правами
	Малое число ревизий (оценки) программных средств	Злоупотребление правами
	Неправильное распределение прав доступа	Злоупотребление правами
	Сложный пользовательский интерфейс	Ошибка в использовании
	Изъяны в документировании	Ошибка в использовании
	Установлен неправильный параметр	Ошибка в использовании
	Некорректные даты	Ошибка в использовании
Компьютерная сеть	Изъяны в механизмах пользовательской идентификации	Подделывание прав
	Незащищенные таблицы паролей	Подделывание прав
	Плохое управление паролями	Подделывание прав
	Запущены не нужные службы	Незаконная обработка данных
	Недоработанное или новое программное обеспечение	Программный сбой
	Изъяны эффективного контроля внесения изменений	Программный сбой
	Неконтролируемая загрузка и использование программного обеспечения	Подделка программного обеспечения
	Изъяны в процедуре резервного копирования	Подделка программного обеспечения
	Изъяны физической защиты здания, дверей, окон	Кража оборудования и документов
	Отказ менеджмента от проверки отчетов	Несанкционированное использование оборудования
	Незащищенные линии связи	Подслушивание
	Незащищенный чувствительный трафик	Подслушивание

	Плохая проводка кабельной системы	Отказ телекоммуникационного оборудования
	Единственная точка отказа	Отказ телекоммуникационного оборудования
	Изъяны идентификации и аутентификации отправителя и получателя информации	Подделывание прав
	Опасная сетевая архитектура	Удаленный шпионаж
	Передача паролей в открытом виде	Удаленный шпионаж
	Неадекватное управление сетью (способность системы противостоять ошибкам маршрутизации)	Насыщенность информационной системы
	Незащищенность подключения общедоступной сети	Несанкционированное использование оборудования
Персонал	Отсутствие персонала	Нарушение доступности персонала
	Недостаточное обучение безопасности	Ошибки в использовании
	Неправильное использование программного обеспечения и оборудования	Ошибки в использовании
	Изъяны в понимании и обязанностях по информационной безопасности	Ошибки в использовании
	Нехватка механизмов мониторинга и контроля	Незаконная обработка данных
	Неконтролируемая работа за внешним штатом, убирающими работниками	Кража оборудования или документов
	Изъяны в правильном использовании носителей передачи данных и обмена сообщениями	Несанкционированное использование оборудования
	Изъяны в процедурах регистрации и де-регистрации, пересмотра прав доступа персонала	Злоупотребление правом
	Изъяны в контроле над средствами обработки	Злоупотребление правом

	информации	
	Нехватка установленных контрольных механизмов в случае нарушения правил безопасности	Кража носителей и документов

Риск – это также уровень воздействия на деятельность библиотеки в целом (включая предназначение, функции, имидж, репутацию), на ее активы, персонал, следующие в первую очередь из-за использования информационной системы, подвергаемой потенциальному воздействию угрозы. Риск является функцией вероятности того, что данный источник угрозы, использует потенциальную уязвимость и осуществит неблагоприятное воздействие на библиотеку.

Информационный риск (IT-риск) – это опасность возникновения убытков в результате обработки, хранения и передачи информации с помощью автоматизированных информационных систем, а также сбоев в работе этих систем.

Значение риска тем выше, чем более уязвимой является существующая система безопасности и чем выше вероятность реализации внутренних и внешних воздействий и угроз. Риск первоначально является категорией неопределенности, которая связана с недостаточностью информации о понимании возможного события, знаний о нем, его последствиями или возможностью возникновения.

Риск возникает тогда, когда существует вероятность, что данный источник опасности использует (случайно или намеренно) конкретную уязвимость системы информационной безопасности. Риски могут возникнуть в основном из-за: неавторизованного (злоумышленного или случайного) раскрытия, изменения или уничтожения информации; непреднамеренных ошибок или упущений; технических сбоев в связи с природными или техногенными катастрофами; недостатка внимания и ошибок при внедрении и эксплуатировании автоматизированной системы библиотеки.

Чрезвычайно важным и сложным является умение управлять рисками информационной безопасности. Управление рисками нормативно закреплено в уже упоминавшемся стандарте ISO/IEC 27005 Информационная технология – Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности.

Процесс менеджмента рисков информационной безопасности состоит из установления контекста, оценки риска, обработки риска, принятия риска, обмена информацией относительно риска, а также мониторинга и пересмотра риска. В основу процесса менеджмента рисков положен *итеративный*

подход, это значит, что оценка и обработка риска идет *итерациями* – отдельными непрерывными шагами. Это увеличивает глубину и детализацию оценки при каждой итерации.

Процесс управления рисками включает в себя идентификацию риска, оценку степени риска, а также осуществления мероприятий, направленных на его уменьшение до приемлемого уровня. Вовремя оценить риск и принять меры для его снижения позволяет руководству библиотеки сбалансировать экономические издержки защитных мер, что позволит обеспечить успешную работу по организации и сохранности всех ее ресурсов.

Цель выполнения процессов управления рисками состоит в том, чтобы дать возможность библиотеке выполнить свою миссию за счёт: повышения безопасности всех своих систем, которые хранят, обрабатывают и передают информацию; повышения осведомленности руководства относительно принятых решений по управлению риском для получения обоснованных объёмов затрат на обеспечение всех систем жизнедеятельности библиотеки; минимизации рисков – принятие мер (технических, операционных) с целью снижения совокупного риска для библиотеки и сокращения возможного ущерба. Риск потери данных, например, может быть снижен путем установки более эффективного антивирусного программного обеспечения; размещения данных на внешнем «облачном хранилище»; отказа от начала или продолжения деятельности, при которой может быть реализован риск и т.д.

Процесс минимизации рисков также включает в себя: выявление возможных проблем и нахождение их решения; определение сроков внедрения новых технологий; оптимизацию библиотечно-информационных процессов и услуг библиотеки; обеспечение защиты информации; обеспечение защиты пользователей информации и персонала библиотеки; разработку стратегии действий при форс-мажорных обстоятельствах; определение фактических потребностей в информационных ресурсах и услугах.

Важно правильно оценить уровни риска в библиотеке:

– *высокий* – источник угрозы является высокоактивным и обладает большими возможностями, а предотвращение уязвимости является неэффективным, что может привести к серьезным потерям информационных активов, нарушить миссию библиотеки;

– с*редний* – источник угрозы достаточно активен и располагает широкими возможностями, средства препятствия уязвимости действуют эффективно, но существует вероятность потери некоторых материальных активов, нанесения вреда репутации библиотеке, что может помешать её работе.

– *низкий* – у источника угроз отсутствуют мотивации для осуществления угроз, а средства противодействия действуют эффективно, что может привести к незначительным потерям ресурсов библиотеки и незначительно помешать ее работе.

Для снижения риска информационной безопасности существует ряд ограничений: временные, финансовые, технические, эксплуатационные, этические, экологические, юридические, квалификация персонала и др.

Тема 3. Методы и средства защиты информации в библиотеке

Для защиты информации и информационных ресурсов в библиотеке используется целый комплекс методов и средств. Каждый метод реализуется с помощью соответствующих средств защиты. Методы и средства выступают в тесной взаимосвязи.

На практике обычно используются следующие *методы защиты*:

– *препятствие* – метод физического преграждения пути злоумышленнику к защищаемым объектам ИБ: библиотеке в целом, аппаратным средствам, носителям информации и т.п. Препятствие создается с помощью технических и программно-технических средств;

– *управление доступом* – метод защиты, реализация которого позволяет регулировать использование всех информационных ресурсов библиотеки. Это происходит путем: проверки полномочий (прав доступа) пользователя в библиотеку и ее информационным ресурсам в соответствии с регламентам; регистрации обращений пользователей к защищаемым ресурсам; реагирования при попытках несанкционированных действий (сигнализация, отказ в запросе или обслуживании);

– *шифрование* или *преобразование данных* с использованием криптографических способов. Шифрование является основой всех систем аутентификации и авторизации пользователей и персонала, средством безопасного хранения данных и защищенного канала компьютерной сети библиотеки;

– *регламентация* – метод защиты информации на основе разработки нормативно-правовых актов, которые бы упорядочивали использование фонда и баз данных библиотеки и сводили несанкционированный доступ к ним к минимуму;

– *принуждение* – метод защиты, при котором пользователи и персонал библиотеки вынуждены соблюдать правила хранения, обработки, передачи и использования защищаемой информации; создание таких условий, при которых необходимо соблюдать их под угрозой административной, материальной и уголовной ответственности;

– *побуждение* – создание условий, которые мотивируют пользователей и персонал библиотеки к должному поведению с соблюдением сложившихся морально-этических норм.

Методы обеспечения информационной безопасности реализуются с помощью следующих основных средств: *физических, аппаратных, программных, аппаратно-программных, криптографических, организационных, законодательных и морально-этических*. Рассмотрим их более детально.

Физические средства защиты информации предназначены для: внешней охраны территории библиотеки и наблюдения за ней, ее здания, внутренних помещений; контролируемого доступа в здание и помещения; охраны оборудования; защиты компонентов автоматизированной библиотечно-информационной системы и других объектов информационной безопасности. К физическим средствам относятся разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий злоумышленникам. Они могут быть механическими, электромеханическими, электронными, электронно-оптическими, радио- и радиотехническими и другими. Предназначены для препятствия несанкционированному доступу (входу, выходу), проноса (выноса) документов, компьютерного и периферийного оборудования и других материальных средств библиотеки.

Физические средства защиты, которые используются в библиотеках, можно разделить на четыре основные группы:

1. С*редства предупреждения:*

– усиленные двери с электронными замками и датчиками, с программируемым временем открывания с помощью механических или электронных часов, которые вызывают сигнал тревоги;

− металлические решетки и датчики на окнах, специальное остекление на основе пластических масс, армированных стальной проволокой;

− сейфы, железные шкафы с надежной двойной системой запирания;

− другое оборудование, защищающее помещения, где находятся носители информации.

2. *Средства контроля доступа,* основываются на двух основных методах – *идентификации* и *аутентификации,* использование которых позволяет исключить неправомерный доступ в библиотеку и к ее информационным ресурсам.

Идентификация – это механизм присвоения собственного уникального имени или образа пользователю, который посещает библиотеку или взаимодействует с ней удаленно с использованием интернета.

Аутентификация – это способ проверки совпадения уникального имени пользователя с тем образом, которому разрешен допуск. Подлинность, как правило, определяется тремя способами: человеком, программой, устройством. При этом объектом аутентификации может быть не только человек, но и техническое средство (компьютер, монитор, носители информации) или данные. Простейший способ защиты – пароль.

Регулирование доступа в здание или помещения библиотеки происходит посредством опознавания службой охраны или техническими средствами. Контролируемый доступ предполагает ограничение круга лиц, допускаемых в определенные защищаемые зоны, помещения, а также отслеживание за передвижением этих лиц внутри них.

Наибольшее распространение в библиотеках получили *атрибутные методы* опознавания и подтверждения полномочий, такие, как: документы (паспорт, удостоверение и др.), пластиковые электронные читательские билеты с фотоизображением, пластиковые карты для персонала библиотеки с магнитными, электрическими идентификаторами. Существует много устройств опознавания и идентификации личности, использующих подобные карты. Одни из них оптическим путем сличают фотографии и другие идентификационные элементы, другие – магнитные поля.

Все устройства идентификации могут работать как отдельно, так и в интегрированном комплексе. Интегрированный подход является многоцелевым и реализуется в АБИС библиотеки, которые позволяют выполнять функции охраны, контроля, регистрации и сигнализации. Такие системы обеспечивают: допуск в здание библиотеки по карточке, содержащей индивидуальный электронный код; блокирование несанкционированного прохода как читателей, так и сотрудников библиотеки (например, нарушителей графика работы – опоздание, преждевременный уход); открытие зоны и регистрация времени свободного выхода через турникеты; обработку полученных данных и формирование различных документов (табелей, ведомостей, списков) о пользователях и сотрудниках в масштабах реального времени и ретроспективно.

3. *Средства обнаружения угроз* – охранная сигнализация, система видеонаблюдения, охранное телевидение, охранное освещение. Эффективность работы *системы охраны и охранной сигнализации* в основном определяется параметрами и принципом работы всевозможных датчиков: механических, ультразвуковых, с инфракрасным излучением, фотоэлектрических и многих других. Датчики посредством тех или иных каналов связи соединены с контрольно-приемным устройством пункта (или поста) охраны и средствами тревожного оповещения. Каналами связи в системах охранной сигнализации могут быть специально проложенные

кабельные линии, телефонные линии, линии связи трансляции, системы освещения. Важным объектом охранной системы являются средства тревожного оповещения: звонки, лампочки, сирены.

Одним из распространенных средств охраны является *охранное видеонаблюдение и телевидение*. Привлекательной особенностью охранного телевидения является возможность не только отметить нарушение режима охраны объекта, но и контролировать обстановку вокруг него, определять опасность действий, вести скрытое наблюдение и производить видеозапись для последующего анализа правонарушения. Источниками изображения (датчиками) в системах охранного телевидения являются видеокамеры и мониторы, которые согласованы по параметрам с видеокамерой.

Составной частью системы защиты любого объекта является *охранное освещение*: дежурное и тревожное. Дежурное освещение предназначается для постоянного использования в нерабочие часы, в вечернее и ночное время, как на территории объекта, так и внутри здания. Тревожное освещение включается при поступлении сигнала тревоги от средства охранной сигнализации. Кроме того, по сигналу тревоги в дополнение к освещению могут включаться и звуковые приборы (звонки, сирены и др.). Сигнализация и дежурное освещение должны иметь резервное электропитание на случай аварии или выключения электроэнергии.

4. *Средства ликвидации угроз,* которые используются в библиотеках, представлены в основном современными *охранно-пожарными системами и системами беспрерывного электропитания.*

Охранно-пожарные системы – это комплекс мер и средств, которые призваны предотвратить возникновения пожара, уберечь здоровье и жизни людей, исключить материальные потери библиотеки. Они включают в себя:

− пожарную сигнализацию, подключенную к МЧС;

− первичные средства пожаротушения (огнетушители на пенной, углекислотной, пенно-воздушной основе);

− систему водоснабжения для ликвидации пожара;

− автоматическую систему пожаротушения, которая приводится в действие в результате срабатывания датчиков и выполняет автономное тушение пожара без участия человека;

− установку преград, препятствующих распространению огня (огнестойкие двери, окна, ворота, устройства автоматического отключения в случае возгорания);

− средства оповещения и эвакуационные пути с надежной защитой от огня и ядовитых газов, оборудование эвакуационных выходов и безопасных зон, где можно находиться во время пожара;

− средства защиты от задымления (вентиляционные устройства, системы отвода воздуха, холодильные установки, кондиционеры), которые при возгорании поставляют охлажденный и чистый воздух в эвакуационные проходы.

Системы бесперебойного электроснабжения представляет собой электроустановку, которая предназначена для автономного электропитания технических устройств библиотеки в случаях отключения (кратковременного нарушения, падения напряжения в сети до критически низкого уровня) электроснабжения от централизованных источников посредством использования альтернативного источника энергии. Время автономной работы такой системы, как правило, соответствует времени завершения функционирования информационно-коммуникационных систем библиотеки без потери информации и повреждений оборудования. В качестве альтернативных источников электроэнергии выступают: электрохимические аккумуляторные батареи, конденсаторы, моторы-генераторы, стабилизаторы переменного напряжения, трансформаторы и другие.

Аппаратные средства защиты информации – это обязательная часть любой автоматизированной информационной системы. В их состав входят электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначены для определения и пресечения (локализации) возможных каналов утечки информации, защиты ее от разглашения, аутентификации пользователей, а также противодействия несанкционированному доступу к источникам информации. Кроме того, аппаратные средства обеспечивают внутреннюю защиту структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д.

По функциональному назначению аппаратные средства могут быть классифицированы на а) средства обнаружения, поиска и детальных измерений, б) средства активного и пассивного противодействия. Для примера, к первым можно отнести группу индикаторов электромагнитных излучений, обладающих широким спектром принимаемых сигналов и довольно низкой чувствительностью, ко вторым – профессиональный комплекс, предназначенный для автоматического обнаружения, определения местонахождения и пеленгования радиопередатчиков, радиомикрофонов, телефонных закладок.

В особую группу выделяются аппаратные средства защиты персональных компьютеров и коммуникационных систем, которые

применяются как в отдельных компьютерах, так и на различных уровнях и узлах компьютерных сетей: в центральных процессорах персональных компьютеров, в их оперативных запоминающих устройствах, контроллерах ввода-вывода, внешних запоминающих устройствах, терминалах и других.

Аппаратные средства защиты применяются также в терминалах пользователей для предотвращения утечки информации. При подключении незарегистрированного пользователя вначале происходит его автоматическая идентификация (определение кода или номера) терминала, с которого поступил запрос и только потом выдается (или блокируются выдача) запрашиваемых данных. В многопользовательском режиме автоматизированной библиотечно-информационной системе идентификации терминала недостаточно. Необходимо осуществить аутентификацию пользователя, то есть установить его подлинность и полномочия. Это необходимо и потому, что разные пользователи системы могут иметь доступ только к отдельным файлам (базам данных), а также ограниченные полномочия их использования.

Программные средства защиты информации предназначены для выполнения логических и интеллектуальных функций защиты информации и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратного обеспечения и контроля. В последнем случае они называются *программно-аппаратными средствами защиты,* в которых программные (микропрограммные) и аппаратные части полностью взаимосвязаны и неразделимы.

Программные средства защиты информации являются наиболее распространенным видом защиты. Они обладают следующими положительными свойствами: универсальностью, гибкостью, простотой реализации, возможностью изменения и развития. Данные свойства делает их одновременно и самыми уязвимыми элементами защиты информационной системы библиотеки. Подробнее об программных средствах информационной безопасности пойдет речь в следующей теме данной учебной дисциплины.

Криптографические средства включают способы обеспечения конфиденциальности информации в компьютерной сети с помощью *шифрования и аутентификации.* Подробнее о криптографии речь пойдет в следующей теме, посвященной безопасности компьютерных систем библиотеки.

Правовое обеспечение защиты информации в Республике Беларусь состоит из трех основных групп: актов национального законодательства, документов государственных органов, государственных стандартов в области

информационной безопасности. Особое значение имеют «Концепция безопасности Республики Беларусь» и «Концепция информационной безопасности Республики Беларусь». Все они составляют законодательную и концептуальную базу для построения системы информационной безопасности библиотек. Правовая регламентация деятельности в области защиты информации в библиотеке имеет целью защиту ее информационных ресурсов, обеспечение прав пользователей на получение легитимной информации, конституционных прав граждан на защиту личных данных.

Нормативно-правовое обеспечение информационной безопасности обеспечивает защиту интересов:

− физических лиц (вводятся нормы, устанавливающие пределы сбора и использования сведений об этих лицах со стороны государства и иных субъектов);

− государства и общества (устанавливает приоритеты защиты информации, охраняемой как собственность государства);

− юридических и физических лиц (имеет нормы, регулирующие обращение с охраняемой информацией и устанавливает механизмы защиты этих субъектов).

Государственная политика Республики Беларусь в области информационной безопасности основывается на следующих принципах: нормативно-правовая база; регламентация доступа к информации; юридическая ответственность за сохранность информации; контроль за разработкой и использованием средств защиты информации; предоставление гражданам доступа к мировым информационным ресурсам.

Основными потенциальными либо реально существующими угрозами национальной безопасности Республики Беларусь в информационной сфере в соответствии с «Концепцией национальной безопасности Республики Беларусь» являются:

– деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;

– нарушение функционирования критически важных объектов информатизации;

– недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;

– снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, национальных информационных ресурсов;

– утрата либо разглашение сведений, составляющих охраняемую законодательством тайну и способных причинить ущерб национальной безопасности.

К нормативно-правовым актам относятся: Конституция Республики Беларусь, законы Республики Беларусь, указы Президента Республики Беларусь, постановления Совета Министров Республики Беларусь, которые регулируют самые различные аспекты в сфере информационных отношений и информатизации, защиты и доступа к информации, персональных данных, авторского права на информацию и т.п.

Законы: «Об информации, информатизации и защите информации», «О защите персональных данных», «Об авторском праве и смежных правах», «Об электронном документе и электронной цифровой подписи». «О переписи населения», «О регистре населения», «О защите персональных данных» и др.

Кодексы, имеющие законодательную силу:

− «*Гражданский кодекс Республики Беларусь»* (содержит нормы, касающиеся служебной и коммерческой тайны, закрепляет такие формы отношений, как информационные услуги, электронную подпись; предусматривает ответственность за незаконное использование информации;

− *«Кодекс Республики Беларусь об административных правонарушениях»* (определяет административно-правовые санкции за правонарушения в информационной сфере, связанные с отказом в предоставлении гражданину информации, непосредственно затрагивающей его права, свободы и законные интересы, несанкционированный доступ к компьютерной информации, нарушение правил защиты информации и др.);

− *«Уголовный кодекс Республики Беларусь»* определяет ответственность за преступления против информационной безопасности, а также иные составы преступлений в информационной сфере (хищение путем использования информационных технологий, умышленное (по неосторожности) разглашение государственной и служебной тайны и др.);

− *«Трудовой кодекс Республики Беларусь»* (устанавливает для работников обязанность хранить государственную и служебную тайну, не разглашать коммерческую тайну нанимателя, коммерческую тайну третьих лиц, к которой наниматель получил доступ);

− *«Налоговый кодекс Республики Беларусь»*; (включает нормы, определяющие порядок защиты различных видов конфиденциальной информации);

− *«Кодекс об образовании Республики Беларусь»;*

− «*Кодекс о культуре Республики Беларусь».*

Указы Президента Республики Беларусь и *постановления Совета Министров* Республики Беларусь представляют собой нормативно-правовые документы, которые можно подразделить на четыре основные группы:

− о защите информации;

− о доступе граждан к информации;

− о компетенции органов государственной власти в сфере защиты информации;

− о международном сотрудничестве в сфере информационной безопасности, включая государства-члены Содружества Независимых Государств.

Среди них:

− *указы Президента* Республики Беларусь: «Об утверждении Концепции национальной безопасности Республики Беларусь» (2010 г.), «Об утверждении Концепции информационной безопасности Республики Беларусь» (2019 г.), «О совершенствовании государственного регулирования в области защиты информации» (2019 г.), «Об особенностях использования национального сегмента сети Интернет» (2019 г.), «Об общегосударственной автоматизированной информационной системе» (2019 г.), «О некоторых мерах по совершенствованию защиты информации» (2013 г.) «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» (2011); «О мерах по совершенствованию использования национального сегмента сети Интернет» (2010 г.) и др.

− *постановления Совета Министров* Республики Беларусь: «О некоторых вопросах интернет-сайтов государственных органов и организаций», «Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) и др.

Отдельное место занимают *постановления и приказы* Оперативно-аналитического центра (ОАЦ) при Президенте Республики Беларусь, среди которых особое внимание заслуживают:

− постановление ОАЦ, Министерства связи и информатизации Республики Беларусь и Министерства информации Республики Беларусь «Об утверждении Положения о порядке ограничения (возобновления) доступа к интернет-ресурсу» (2018 г.);

− приказы ОАЦ – «Об утверждении Положения о порядке проведения государственной экспертизы средств технической и криптографической защиты информации» (2013 г.), «О подтверждении соответствия средств защиты информации» (2020 г.), «О технической и криптографической защите персональных данных» (2021 г.), «Об обучении по вопросам защиты персональных данных» (2021 г.) и др.

Административные средства защиты информации представляют собой действия, предпринимаемые руководством библиотеки для обеспечения информационной безопасности. К ним относятся: правила внутреннего распорядка библиотеки, режим работы сотрудников,

должностные инструкции, руководства пользователей компьютерной сети, правила использования интернет, правила приобретения средств безопасности, правила использования лицензионных программных продуктов и информационных ресурсов и др.

Морально-этические средства защиты информации основываются на нормах, которые сложились в стране в целом и в библиотеке, в частности. К ним относятся меры воспитательного характера, связанные с формированием у пользователей компьютерных систем и сетей следующих моральных норм:

− недопустимость нарушения конфиденциальности, целостности информации, препятствия открытому доступу к информационным ресурсам библиотеки;

− использования чужих информационных ресурсов;

− бережного отношения к компьютерной технике и сетевому оборудованию и т.д.

Очень важно проводить в библиотеке воспитательные мероприятия по противодействию пиратскому копированию информации и программных средств, внедрять в сознание пользователей и сотрудников библиотеки аморальность всяческих покушений на нарушение конфиденциальности, целостности и доступности информационных ресурсов, несанкционированного доступа к автоматизированной системе библиотеки, нарушения авторских прав и защиты личных данных.

В заключение отметим, что использование какого-либо одного из выше рассмотренных методов и способов защиты информации в библиотеке не обеспечит надёжной защиты ее информационных ресурсов и информационной безопасности в целом. Необходим системный подход. Это обеспечивается на уровне *политики информационной безопасности* библиотеки, которая представляет собой совокупность документированных административных, организационных, технологических и процедурных решений по обеспечению защиты ее информационно-коммуникационной инфраструктуры.

Тема 4. Информационная безопасность компьютерных систем библиотеки

Понятие. Безопасность компьютерных систем и сетей – сложная научно-прикладная проблема, является подразделом компьютерной безопасности, которая в свою очередь − частью информационной безопасности. Она имеет законодательные, нормативные, программно-технические, организационные, информационно-психологические, морально-

этические и другие аспекты. В этой теме речь пойдет преимущественно о средствах защиты локальных компьютерных систем, в том числе и в библиотеках.

Под термином ***«безопасность компьютерных систем библиотеки»*** будем понимать комплекс процедур, стандартов, правил и средств, призванных обеспечить их безопасность.

Объектами защиты в библиотечных компьютерных системах и сетях являются, хранящиеся в них и передающиеся по сети, информационные ресурсы, компьютеры и сетевое оборудование, а также пользователи сети.

Безопасная компьютерная сеть библиотеки – это система, которая: 1) защищает данные (информационные ресурсы) от несанкционированного доступа; 2) всегда обеспечивает доступ пользователей; 3) надежно хранит информацию, обеспечивает целостность данных. Другими словами, она обладает *свойствами конфиденциальности, доступности и целостности.* Некоторые специалисты называют их требованиями, которые предъявляются к компьютерным системам и коммуникациям, но это, по сути, не меняет их понятийное поле.

Конфиденциальность компьютерной системы заключается в том, что информация, которая находится в ее базах данных, будет доступна только авторизованным пользователям, т.е. тем, которым разрешен доступ. За исключением случая, когда информация осознанно предоставляется широкому кругу людей, например, на сайте библиотеки, в локальном и онлайн доступе к электронному каталогу и т.п.

Целостность компьютерной системы – гарантия сохранности данных, которая обеспечивает невозможность изменять их, модифицировать и разрушать. Если этого не сделать, то злоумышленник может, например, изменить данные на сервере, испортить коды свободного программного обеспечения и нанести этим ущерб библиотеке.

Доступность компьютерной системы – гарантия того, что только авторизованные пользователи всегда получат доступ к данным. В противном случае, злоумышленником могут быть предприняты действия, в результате которых, помещенные на сервер данные станут недоступными для тех, кому они предназначены в результате его блокировки.

Понятия конфиденциальности, целостности и доступности относятся не только к информации, но и к программно-техническим ресурсам системы: компьютерам, периферийному оборудованию, сетевым устройствам, приложениям. Их несанкционированное использование может привести к нарушению безопасности системы. Угроза целостности компьютерной сети библиотеки заключается в том, что злоумышленник может изменить параметры настройки устройств, маршрутизацию потока данных, физически

повредить оборудование и т.п. Свойство *целостности* заключается в неизменности параметров настройки всех компонентов сети. *Конфиденциальность* проявляется в том, что доступ к устройству системы должны иметь только те пользователи, которым он разрешен, выполнять они могут только те операции с устройством, которые для них определены. Свойство *доступности* компонентов системы реализуется через их постоянную готовность к использованию пользователями, когда в этом возникает необходимость. Все отмеченное, непосредственно влияет на безопасность системы в целом, а не санкционированные, например, отправка факсов, электронной почты, распечатка текстовых файлов, доступ в интернет и т.п. приведет к материальному ущербу библиотеке и ее информационной безопасности.

Угрозы компьютерной системе – это действия, направленные на нарушение конфиденциальности, целостности, доступности информации, а также на нелегальное использование программно-технических ресурсов сети. Реализованная угроза на компьютерную систему библиотеки называется *атакой*. Каждая угроза проявляется через понятие *риска.*

Риск – это вероятностная оценка величины возможного ущерба, который может понести библиотека при успешно проведенной атаке на компьютерную сеть. Значение риска тем выше, чем более уязвимой является существующая система безопасности и чем выше вероятность реализации атаки. Риск первоначально является категорией неопределенности, которая связана с недостаточностью информации о понимании возможного события, знаний о нем, его последствиями или возможностью возникновения.

Чрезвычайно важным и сложным является умение управлять рисками информационной безопасности. Управление рисками, как уже отмечалось в теме 2 нормативно закреплено в стандарте ISO/IEC 27005. В приложении D выше названного стандарта приводятся примеры угроз безопасности информационным технологиям в отношении аппаратных средств, программного обеспечения, собственно компьютерной сети, пользователей и сайтов организации. В Таблице 2. на основании стандарта приведены возможные виды угроз вышеназванным объектам безопасности компьютерной сети.

Источники угроз безопасности сети можно подразделить на следующие группы:

1) связанные *с человеческим фактором,* среди которых – *внешние* (действия кибер-преступников, хакеров, интернет-мошенников, недобросовестных партнеров, криминальных структур) и *внутренние* (действия персонала сети);

2) связанные *с техническим фактором* (использование физического и морально устаревшего оборудования, некачественных программно-аппаратных средств, помехи в линиях связи и др.);

3) связанные со *стихийным факторами* (природные катаклизмы, стихийные бедствия).

Табл. 2. Виды угроз объектам безопасности компьютерной сети.

Объект	Примеры угроз
Аппаратные средства	Нарушение ремонтопригодности информационной системы Разрушение оборудования или носителей Пыль, коррозия, обледенение Электромагнитная радиация Ошибка в использовании Потеря источника питания Метеорологическое явления Кража носителей или документов
Программное обеспечение	Злоупотребление правами Искажение данных Ошибки в использовании
Сеть	Подделывание прав Незаконная обработка данных Программный сбой Подделка программного обеспечения Кража носителей или документов Несанкционированное использование оборудования Отрицание действий Подслушивание Подделывание прав Удалённый шпионаж Перенасыщенность информационной системы Несанкционированное использование оборудования
Пользователи	Нарушение доступности персонала Уничтожение оборудования или носителей Ошибка в использовании Незаконная обработка данных Кража носителей или документов

	Несанкционированное использование оборудования
Сайт	Уничтожение оборудования Уничтожение носителей информации Нестабильная мощность сетей Потеря источника питания Кража оборудования Злоупотребление правами

бедствия, аварийные ситуации с отключением электропитания и прочие форс-мажорные обстоятельства). Все три источника угроз необходимо обязательно учитывать при организации системы безопасности сетей.

Угрозы компьютерной сети бывают также ***умышленные и неумышленные.***

Умышленные угрозы **–** это пассивное или активное негативное воздействие на целостность и доступность информации, а также приведение в нерабочее состояние программных средств и устройств. Как уже отмечалось, это приводит к нанесению ущерба библиотеке.

В компьютерных сетях выделяют следующие ***типы умышленных угроз***:

1. *Незаконное проникновение* в один из компьютеров сети под видом легального пользователя. Это может достигаться через уязвимые места операционных систем, связанных с ошибками безопасности памяти или их нелицензионностью (подлинностью). Злоумышленник может «обойти» стандартную систему безопасности входа в сеть. Самые серьезные из этих ошибок могут дать сетевым злоумышленникам полный контроль над компьютером.

2. *Использование «чужих» паролей*. Злоумышленник может получить их путем «подглядывания», расшифровки файла паролей, подбора паролей, получения пароля путем анализа сетевого трафика. Подбор паролей может выполняться с использованием специальных программ, которые работают путем перебора слов из некоторого файла, содержащего большое количество слов. Файл формируется с учетом психологических особенностей человека, который часто применяет в качестве пароля легко запоминаемые слова, буквенные сочетания, символы и цифровые значения. Наиболее опасно незаконное проникновение под паролем администратора сети. Поэтому очень важно, чтобы все пользователи сети сохраняли свои пароли в тайне, а также выбирали наиболее сложные пароли.

3. Путем внедрения в чужой компьютер вредоносной программы − *«троянского коня»*. Она выполняет алгоритм действий, заданный

злоумышленником, считывает коды пароля, вводимого пользователем. Эта вредоносная программа всегда проникает в компьютер сети под видом легитимного программного обеспечения (приложения, полезной утилиты, игры и т.д.). Она *«маскируется»* под эти программы, заражает другие файлы, производит разрушение системы, приводит к полной или частичной утрате информации.

4. *Несанкционированные действия легального пользователя.* Они заключатся в том, что пользователи сети (например, администраторы) выполняют в ней действия, которые выходят за пределы их должностных обязанностей. Имея неограниченные права доступа ко всем ресурсам сети, они могут воспользоваться информацией, доступ к которой им запрещен. Имеет статистика, которая показывает, что примерно половина всех попыток нарушения безопасности сети исходит от самих ее легальных пользователей. Здесь появляются морально-этические проблемы безопасности сетей.

5. *«Прослушивание» внутрисетевого трафика* – это незаконный мониторинг сети, перехват данных, передаваемых по линиям связи, и анализ сетевых сообщений. Для «прослушивания» используются доступные программные и аппаратные анализаторы трафика. Особенно такой тип угрозы присущ безопасности интернета, который имеет глобальные сетевые связи и которые значительно труднее защитить, чем в локальных компьютерных сетях. Однако, и локальные сети функционируют также с использованием технологии интернета, что еще более увеличивает опасность несанкционированного входа в их узлы.

6. *Фишинг (phishing, выуживание)* – один из видов интернет-мошенничества, получивший широкое распространение. Его цель заключается в получении доступа к конфиденциальным данным пользователей – логинам и паролям. Для этого используется массовые рассылки электронных писем от имени популярных брендов, личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на поддельный сайт, внешне неотличимый от настоящего либо на сайт с редиректом (автоматическим перенаправлением посетителя на другой ресурс). Как только пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить его ввести свой логин и пароль. В результате они могут получить доступ к определённому сайту, аккаунту или банковским счетам.

Фишинг базируется на незнании пользователями основ сетевой безопасности, в частности, того, что распространенные сервисы не рассылают писем с просьбами сообщить им свои учётные данные, пароли и

прочее. Для защиты данных новые версии браузеров уже обладают возможностями *«антифишинга»*.

7. *Компьютерные вирусы* – вредоносное программное обеспечение, которое способно внедриться в код других программ, а также в системные области памяти компьютера, загрузочные секторы. Его цель – распространение своих копий по каналам связи. Это может привести к нарушению работы программно-аппаратных комплексов, сбоям в работе компьютеров, периферийного оборудования, сетевых устройств, накопителей информации и т.п.; к удалению файлов и, даже, операционной системы; негодности структуры размещения данных; блокированию работы пользователей сети и т.д. Вирусы распространяются самопроизвольно.

Основные виды компьютерных вирусов: *трояны* и *«сетевые черви»*.

Как уже отмечалось, *«троян»* представляет собой разновидность вредоносной компьютерной программы. Имеется, по меньшей мере, пять основных типов троянов: удаленный доступ, уничтожение данных, загрузчик, деактиватор программ безопасности и сервер. Трояны являются частью различных вложений в электронных письмах или ссылках на скачивание. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина. Он не заражает другие программы или данные. Трояны не способны самостоятельно проникать на компьютеры, а распространяются злоумышленниками под видом «полезного» программного обеспечения. Но вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

«Сетевой червь» является самой опасной разновидностью вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети. Его распространение происходит по причинам уязвимости и ошибок в программном обеспечении и администрирования сети, недостатков в пользовательском интерфейсе. «Черви» способны «расползаться» автономно, выбирая и атакуя компьютеры в полностью автоматическом режиме. Скорость распространения сетевого червя зависит от многих факторов: от топологии сети, алгоритма поиска уязвимых компьютеров, средней скорости создания новых копий. Наиболее стремительно они распространяются с использованием протокола TCP/IP – с любого IP-адреса на любой другой.

8. *DoS-атака (DoS, Denial of Service, «отказ в обслуживании»)* – хакерская атака на сервер локальной сети с целью вывести его из строя и получить доступ к предоставляемым системным ресурсам. В настоящее время DoS-атаки наиболее распространены, так как позволяют довести до отказа практически любую систему, не оставляя юридически значимых улик.

Неумышленные угрозы связаны с ошибочными действиями персонала сети, их низкой квалификацией или безответственностью, а также с ненадежностью и отказоустойчивостью программно-технических средств сети, отсутствием лицензий на их использование

Средства и методы защиты компьютерных систем и сетей.

Технические средства защиты – это электрические, электромеханические, электронные и другие типы устройств, которые встраиваются в аппаратуру локальных сетей по стандартному интерфейсу, а также физические – автономные устройства и системы охранной сигнализации и видеонаблюдения, системы противопожарной безопасности, замки на железных дверях, решётки на окнах и т.п.

Программные средства защиты являются основным средством безопасности. Это специально разработанные программы для идентификации пользователей, контроля доступа, шифрования информации. Они также удаляют остаточную (рабочую) информацию типа временных файлов, осуществляют тестовый контроль системы защиты и др. К их *преимуществам относят:* универсальность, гибкость, надежность, простату установки, способность к модификации и развитию; к недостаткам: высокая чувствительность к случайным или преднамеренным изменениям сети, зависимость от типов компьютеров и других аппаратных средств.

Существуют следующие ***виды программных средств защиты*** локальных сетей:

1. ***Средства архивации данных*** – предназначены для объединения нескольких файлов и каталогов в единый файл – *архив* путем осуществления процедуры сжатия и *шифрования данных*, устранения избыточности, но без потерь информации, и с возможностью точного восстановления исходных файлов. Для создания архивов используются *программы-архиваторы*.

2. ***Антивирусные программы*** – большое разнообразие программ, разработанных для обнаружения и защиты информации сетей от компьютерных вирусов, восстановления зараженных файлов и профилактики заражения (модификации) файлов или операционной системы вредоносным кодом.

Для защиты от вирусов используются три *группы методов:*

− *метод анализа содержимого файлов* – основан на поиске в файлах уникальной последовательности байтов – *сигнатуры*, характерной для определенного вируса, а также на проверке целостности и сканировании подозрительных программ. Специалистами антивирусной лаборатории выполняется анализ кода, на основании которого определяется *сигнатура* (характеристика) вируса и помещается в специальную базу данных, с которой работает антивирусная программа. При обнаружении нового вируса

должна создаваться и новая сигнатура в БД антивирусной программы, т.е. необходима постоянная актуализация. *Контроль целостности* основывается на том, что любое неожиданное и беспричинное изменение данных на диске является подозрительным событием, требующим особого внимания антивирусной системы. Факт изменения данных устанавливается путем сравнения контрольной суммы (дайджеста), заранее подсчитанной для исходного состояния тестируемого кода, и контрольной суммы (дайджеста) текущего состояния тестируемого кода. Если они не совпадают, значит, целостность нарушена. *Сканирование подозрительных команд* основано на выявлении в сканируемом файле некоторого числа подозрительных команд и соответствующих кодов. После этого делается предположение о вредоносной сущности файла и его проверка;

−*метод отслеживания поведения программ* основан на анализе поведения запущенных программ, сравнимый с поимкой преступника «за руку» на месте преступления. Он заключаются в протоколировании всех событий, угрожающих безопасности системы и происходящих при реальном выполнении проверяемого кода, либо при его программной *эмуляции (имитации)* функций. Имитация позволяет запускать тестируемую программу в искусственно созданной (виртуальной) среде, которую часто называют «*песочницей*» без опасности повреждения информационного окружения. Использование методов анализа поведения программ показало их высокую эффективность при обнаружении как известных, так и неизвестных компьютерных вирусов;

− *метод регламентации порядка работы* с файлами и программами; он относится к административным мерам обеспечения безопасности компьютерных сетей;

Классификацию антивирусных программ можно представить по следующим основным группам признаков:

− *по размещению в оперативной памяти: резидентные* (работают при запуске операционной системы), находятся в памяти компьютера и осуществляют автоматическую проверку файлов), *нерезидентные* (запускаются по требованию пользователя или по расписанию);

− *по способу защиты от вирусов:*

- *программы-сканеры* (находят вирусы в оперативной памяти, на внутренних и внешних носителях, выводят об этом сообщение); *программы-доктора*, находят зараженные файлы и «лечат» их (Norton AntiVirus, Doctor Web, Kaspersky Antivirus и др.);
- *программы-вакцины,* выполняют иммунизацию системы (файлов, каталогов), блокируя действие вирусов;

- *программы-ревизоры* – запоминают исходное состояние программ, каталогов, системных областей диска до момента инфицирования компьютера, а затем сравнивают текущее состояние с первоначальным, выводя найденные изменения на дисплей);
- *программы-мониторы,* начинают свою работу при запуске ОС, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов по принципу «здесь и сейчас»;
- *программы-фильтры* (сторожа) обнаруживают вирус на ранней стадии, пока он не начал размножаться.

В настоящее время на рынке распространяются *лжеантивирусы*, которые на самом деле не являются антивирусными программами и предназначены для обмана пользователей и получения прибыли. Необходимо уметь отличать их как вредоносное программное обеспечение.

Межсетевые экраны *(брандмауэр или файрвол)* – программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Его *цель* – защита сегментов сети от несанкционированного доступа в протоколах сетевой модели OSI и в программном обеспечении, установленном на компьютерах сети. Межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами. Он защищает от вирусных атак как извне, так и между различными сегментами внутри сети, что повышает ее уровень безопасности. Межсетевые экраны выполняют над поступающим трафиком одну из двух операций: пропустить пакет далее или отбросить пакет.

В соответствии с моделью OSI различают следующие *типы межсетевых экранов*:

– *управляемые коммутаторы*, осуществляют фильтрацию трафика между сетями или узлами сети на канальном уровне и разделяют трафик в рамках локальной сети. Но они не могут быть использованы для обработки трафика из внешних сетей интернета. При реализации политики безопасности в рамках корпоративной сети, основу которых составляют управляемые коммутаторы, они могут быть мощным и достаточно дешёвым решением;

– *пакетные фильтры,* функционируют на сетевом уровне и контролируют прохождение трафика на основе информации, содержащейся в заголовке пакетов. Многие межсетевые экраны данного типа могут оперировать заголовками протоколов и более высокого, транспортного, уровня (например, TCP). Пакетные фильтры остаются самым распространённым типом межсетевых экранов. Данная технология реализована в подавляющем большинстве маршрутизаторов и в некоторых

коммутаторах. При анализе заголовка сетевого пакета могут использоваться следующие параметры: IP-адреса источника и получателя; тип транспортного протокола; поля служебных заголовков протоколов сетевого и транспортного уровней; порт источника и получателя. Пакетные фильтры могут быть реализованы в следующих компонентах сетевой инфраструктуры: пограничные маршрутизаторы; операционные системы; персональные межсетевые экраны.

– *шлюзы сеансового уровня* гарантируют, что ни один сетевой пакет не будет пропущен, если он не принадлежит ранее установленному соединению. Так как межсетевой экран данного типа исключает прямое взаимодействие между двумя узлами, шлюз сеансового уровня является единственным связующим элементом между внешней сетью и внутренними ресурсами. Шлюз сеансового уровня предотвращает возможность реализации DoS-атаки, присущей пакетным фильтрам. Недостаток шлюза, как и во всех выше перечисленных типов межсетевых экранов, – отсутствие возможности проверки содержания поля данных, что позволяет злоумышленнику передавать «троянских коней».

– *посредники прикладного уровня* также исключают прямое взаимодействие двух узлов, однако они способны «понимать» контекст передаваемого трафика. Межсетевые экраны этого типа содержат несколько *приложений-посредников* (*application proxy*), каждое из которых обслуживает свой прикладной протокол. Такой межсетевой экран способен выявлять в передаваемых сообщениях и блокировать команды DoS-атак, проверять сертификаты криптографии конкретного центра, а также определять тип передаваемой информации. Последнее позволяет, например, заблокировать вредоносные сообщения по электронной почте. Недостатками данного типа межсетевых экранов являются большие затраты времени и ресурсов на анализ каждого пакета;

– *инспекторы состояния*, собрали в себе преимущества предыдущих типов в один межсетевой экран, который с высокой производительностью и защищённостью осуществляет фильтрацию трафика с сетевого по прикладной уровень. *«Инспектор»* позволяет контролировать: каждый передаваемый пакет на основе таблицы правил; каждую сессию на основе таблицы состояний; каждое приложение на основе разработанных посредников.

Узким местом межсетевого экрана является то, что он фильтрует только тот трафик, который способен понимать. Существует ряд протоколов, которые используют криптографию, шифруют данные прикладного уровня, из-за чего фильтровать трафик на основании информации, содержащейся на сетевом уровне, становится невозможно.

Прокси-сервера *(proxy, доверенность, доверенное лицо)* – это промежуточный сервер, который является *посредником* между пользователем и сервером баз данных. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, e-mail), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного хранилища быстрого доступа в памяти компьютера (*кэша*, *cache*), если он у него есть. *Кэширование данных* – процесс складирования информации в *кэш* с последующим быстрым извлечением. Запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях.

Прокси-сервер позволяет защищать компьютер клиента от некоторых сетевых атак и помогает сохранять анонимность клиента, но также может использоваться мошенниками для скрытия адреса сайта, уличённого в мошенничестве, изменить (подменить) содержимое целевого сайта, а также перехватить запросы самого пользователя. При этом необходимо учитывать, что при использовании прокси-сервера весь прямой трафик сетевого/транспортного уровней между локальной и глобальной сетями блокируется полностью. Выход из локальной сети в глобальную происходят через прокси-сервер. Доступ из глобальной сети в локальную сеть становятся невозможными в принципе. Необходимо помнить, что использование прокси-сервера не даёт достаточной защиты против атак на более высоких уровнях OSI, например, на уровне приложения.

Криптографические средства – это средства защиты с помощью преобразования информации (шифрования). Криптография – это область научно-практической деятельности об обеспечении секретности или аутентичности (подлинности) передаваемых информационных сообщений. Готовое к передаче сообщение – будь то данные, речь либо графическое изображение документа, обычно называется открытым. Для предотвращения несанкционированного доступа к сообщению оно шифруется, преобразовывается в шифрограмму или закрытый текст. Другими словами, шифрование – это процесс криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.

Криптографические преобразования используются для предотвращения угроз информационной безопасности при реализации следующих сервисов:

– собственно шифрование (обеспечение конфиденциальности данных), что предотвращает утечку информации, а отсутствие ключа у «злоумышленника» не позволяет раскрыть зашифрованную информацию;

– контроль целостности данных с использование алгоритмов несимметричного шифрования и хеширования. *Хеширование* заключается в алгоритмическом преобразовании входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются *хеш-функциями* или функциями свёртки, а их результаты называют *хешем, хеш-кодом* или сводкой сообщения. Все это делает возможным создание определенного способа контроля целостности информации.

– аутентификация пользователей информации в распределенных информационных системах и обеспечение доступа к ним.

Задача криптографической защиты информации заключается в преобразовании информационных объектов с помощью некоторого обратимого математического алгоритма. В процессе шифрования используются следующие параметры: объект – открытый текст и объект – ключ, а результат преобразования – объект – зашифрованный текст. При дешифровании выполняется обратный процесс. Авторизованный и санкционированный пользователь информационной системы, получив сообщение, дешифрует его посредством обратного преобразования криптограммы и получает исходный открытый текст.

Процессу шифрования соответствует специальный алгоритм, при реализации которого используется уникальное числовое значение – *ключ*. Владение ключом позволяет выполнить обратное преобразование и получить открытое сообщение. Стойкость криптографической системы определяется используемыми алгоритмами и степенью секретности ключа.

Различают два основных способа шифрования: *симметричное шифрование* (шифрование с закрытым ключом) и *ассиметричное шифрование* (шифрование с открытым ключом). Симметричное шифрование основывается на использовании одного и того же секретного ключа для шифрования и дешифрования. Ассиметричное заключается в том, что для шифрования используется один общедоступный ключ, а для дешифрования – другой, являющийся секретным, при этом знание общедоступного ключа не позволяет определить секретный ключ.

Средства криптографии используются также в создании еще одного способа защиты информации – *электронной подписи.* Электронная подпись – это некая последовательность символов, которая получена в результате преобразования исходного документа (или любой другой информации) при помощи специального программного обеспечения. Электронная подпись используется в электронном документообороте библиотеки, добавляется при его пересылке к исходному документу. Любое изменение исходного документа делает электронную подпись недействительной.

Выделяют *простую* и *усиленную* электронную подпись. Первая электронная подпись, состоящая из кодов, паролей или иных средств, подтверждает факт ее создания определенным лицом. Вторая (усиленная) – формируется в результате криптографического преобразования информации с использованием ключа электронной подписи. Она позволяет определить лицо, подписавшее электронный документ, обнаружить факт внесения изменений в него после подписания и создается с использованием специальных средств электронной подписи. Имеется ключ проверки электронной подписи, который указывается в квалифицированном сертификате. Требования к электронной подписи сформулированы в Законе Республики Беларусь «Об электронном документе и электронной цифровой подписи» (2009 г.).

Процесс криптографии регламентируется в государственных стандартах Республики Беларусь, посвященных информационным технологиям и безопасности. А именно: криптографические алгоритмы шифрования и контроля целостности; синтаксис криптографической информации для токенов**;** интерфейс обмена информацией с аппаратно-программным носителем криптографической информации (токеном); криптография на основе алгоритма RSA; алгоритмы хэширования; процессы формирования и проверки электронной цифровой подписи и других.

Средства идентификации и аутентификации позволяют с помощью *идентификатора* установить подлинность пользователя, который подключается к компьютерной сети, проверить его права доступа к ней. Аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдаёт. А идентификация обеспечивает выполнение функций установления подлинности и определение полномочий субъекта при его допуске в сеть, контролирования установленных полномочий в процессе сеанса работы, регистрации действий и др.

Средства управления доступом – предназначены для ограничения и регистрации входа-выхода посетителей библиотеки через «точки прохода»;

Протоколирование и аудит – обеспечивает сбор и накопление информации о событиях, происходящих в системе, а также анализ накопленной информации. Целью компьютерного аудита является контроль соответствия компьютерной сети в целом, персональных компьютеров, сетевого оборудования требуемым правилам безопасности и стандартам. Аудит обеспечивает анализ всего, что может относиться к проблемам безопасности сети, а также того, что нужно сделать, чтобы повысить ее безопасность.

Организационные средства защиты состоят из *организационно-технических* (подготовка помещений с компьютерами, прокладка кабельной

системы с учётом требований ограничения доступа к ней и др.) и *организационно-правовых* (законодательство Республики Беларусь и правила работы, устанавливаемые руководством конкретной библиотеки). Они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в компьютерной сети, имеют неограниченные возможности модификации и развития.

Законодательные средства защиты — это законы, постановления правительства и указы президента, нормативные акты и стандарты в области информационной безопасности, которыми регламентируются правила использования и обработки информации, доступа к ней, а также вводятся меры ответственности за нарушения этих правил. Правовая регламентация деятельности в области защиты информации в библиотеке имеет целью защиту ее информационных ресурсов, обеспечение прав пользователей на получение легитимной информации, конституционных прав граждан на защиту личных данных.

Нормативно-технические средства защиты – представляют собой комплекс стандартов Республики Беларусь по безопасности информационных технологий.

Они посвящены:

− критериям оценки безопасности (общей модели, функциональным требованиям безопасности, гарантийным требованиям безопасности);

− требованиям к защите информации;

− методам и средствам безопасности;

− программным средствам защиты от воздействия вредоносных программ;

− профилям защиты (операционной системы сервера, программным средствам маршрутизатора и коммутатора корпоративных сетей; электронной почты);

− процедуре выработки и проверки электронной цифровой подписи;

− устойчивости оборудования;

− испытанию программных продуктов;

− криптографической защите;

− и другим объектам безопасности информационных технологий.

Административные средства защиты – представляют собой действия, предпринимаемые руководством библиотеки для обеспечения компьютерной безопасности. К ним относятся: режим работы сотрудников с автоматизированной системой библиотеки, правила использования интернет, правила эксплуатации компьютерной техники, периферийных устройств, правила использования лицензионных программных продуктов, электронных информационных ресурсов и др.

Морально-этические и психологические средства защиты основываются на нормах, которые сложились в стране в целом и в библиотеке, в частности, в использовании информационно-коммуникационных технологий. К ним относятся меры воспитательного характера, связанные с формированием у пользователей компьютерных систем и сетей следующих моральных норм: недопустимость нарушения конфиденциальности, целостности информации, препятствия открытому доступу к сети; использования чужих программных, «серых» программных продуктов и ресурсов; бережного отношения к компьютерной технике, переферийному и сетевому оборудованию сети и т.д.

Необходим системный подход к безопасности компьютерной системы библиотеки. Как уже отмечалось в Теме 3., это также обеспечивается на уровне *политики информационной безопасности* всей библиотеки.

Тема 5. Информационно-психологическая безопасность пользователей библиотек

В настоящее время библиотековеды только начинают глубоко разрабатывать вопросы поиска направлений и средств обеспечения информационно-психологической безопасности пользователей. Публикации на эту тему рассматривают информационно-психологическую безопасность в контексте развития библиотек в информационном обществе, формирования информационной культуры, библиотерапевтической деятельности. В зарубежных публикациях акцент делается на перенасыщение пользователей библиотек информацией и негативными психологическими эффектами данного явления, а также на развитие информационной грамотности пользователей.

Информационно-психологическая безопасность (ИПБ) является одной из важнейших составляющих информационной безопасности в целом. Информационно-психологическую безопасность в общем виде можно *определить* как состояние защищенности индивидуальной, групповой и общественной психологии от разрушительного воздействия на сознание недоброкачественной информации, что несёт угрозу интеллектуальному, духовно-нравственному состоянию человека, а также его физическому здоровью.

Обеспечение ИПБ должно решаться на уровне государства, общества и на уровне самой личности. В «Концепции информационной безопасности Республики Беларусь» подчеркивается, что *главная цель* обеспечения безопасности информационно-психологической компоненты информационной сферы состоит в сохранении информационного суверенитета и проведения политики информационного нейтралитета, а

также формирование устойчивого иммунитета против деструктивных информационно-психологических воздействий на массовое общественное сознание, а в необходимых случаях – и противодействие им.

Существует множество *угроз информационно-психологической безопасности* и проявляться они могут через СМИ, информационно-коммуникационные технологии, интернет, воспитание, образование, личное общение и т.д. путем воздействия «вредоносной» информации.

Выделяют несколько *видов вредоносной информации*, (фальсифицированной, недостоверной, запрещенной) могущей нанести серьёзный вред психике человека:

– информацию, возбуждающую социальную, расовую, национальную или религиозную ненависть и вражду;

– призывы к войне, экстремистской деятельности или содержащей призывы к такой деятельности;

– пропаганда насилия и жестокости;

– пропаганда ненависти, вражды и превосходства;

– распространение порнографии;

– информация о потреблении наркотических средств и им подобных веществ;

– посягательство на честь, доброе имя и деловую репутацию людей;

– рекламу (недобросовестную, недостоверную, неэтичную, заведомо ложную);

– другую деструктивную информацию.

Развитию информационно-психологических угроз способствуют *информационные факторы*: лавинообразный рост всех видов информации («информационный взрыв»); бурное развитие информационно-коммуникационных средств передачи информации; цифровизация общества. Все это привело к перенасыщению информационной среды, повлияло на восприятие информации человеком. Перепроизводство информации приводит к болезни, которую Элвин Тоффлер назвал *футорошоком* или *информационным стрессом* – неспособности личности воспринимать огромные массивы информации и принимать необходимые решения.

Однако, не вся информация может привести к информационному стрессу, а лишь та, которая является недоброкачественной, перечень которой представлен выше. Эта информация «загрязняет» информационное пространство. Представитель концепции *информационной экологии* Б.Мильтон утверждает, что информация является лишь сырьем, которое позволяет генерировать знания, и что решения принимаются не на основе информации, а на основе знаний, мудрости, интуиции, понимания. Информационно-психологическая угроза, подчеркивает он, возникает только

тогда, когда человек не умеет критически отсеивать, отбирать и перерабатывать информацию, превращать ее в интеллектуальный продукт (знания).

Информационно-психологическое воздействие − информационное, психотронное или психофизическое воздействие на психику человека, оказывающее влияние на восприятие им реальной действительности, в том числе на его поведенческие функции, а также в некоторых случаях на функционирование органов и систем человеческого организма.

Фейковая информация (новости) **–** это поддельная, ложная, фальшивая информация, имеющая, как правило, намеренное распространение в социальных масс-медиа и традиционных СМИ. Цель такой информации – ввести в заблуждение ее потребителей для того, чтобы получить финансовую или политическую выгоду. Авторы поддельных новостей часто используют броские заголовки или полностью сфабрикованные истории для увеличения читательской аудитории и цитируемости. Эти заголовки характеризуются определенными языковыми особенностями: сенсационностью, провокационностью, двусмысленностью, противоречивостью, которые должны привлечь читателя.

Фейковая информация часто рассылается по электронной почте и выступает в данном случае как элемент или разновидность *фишинга*. Такие письма содержат неправдивую информацию сенсационного характера, их задача – спровоцировать адресата перейти по ссылке, а затем заразить его компьютер вредоносной программой.

Прибыль от фейковой информации формируется аналогично доходам от рекламы и генерируется независимо от достоверности опубликованных материалов. Фальшивые новости составляются (фабрикуются) для обмана читателя, с целью увеличения трафика социальных сетей, тиража печатных СМИ и прибыли. Их распространению содействует политическая поляризации общества и возможность быстрого распространения с помощью интернет. Часто такие новости публикуются анонимными или выдуманными авторами, что затрудняет их законное преследование за дезинформацию и/или клевету.

Библиотечные работники должны владеть умениями разоблачения фейковой информации, чтобы в дальнейшем, используя различные методы и формы, транслировать их пользователям библиотеки, формировать у них информационную культуру.

В этом деле будет полезной методика Международной федерации библиотечных ассоциаций и учреждений (ИФЛА). Комитет по свободному доступу к информации и свободе выражения (FAIFE) этой организации

предлагает 8 способов отличить фейковую информацию (новости) от достоверных в Интернете:

1. *Изучите источник новости.* Для этого необходимо зайти на сайт-первоисточник новости и внимательно изучить его – что за сайт, какое его назначение, цель; найти данные о регистрации, сотрудниках, контактную информацию. Нужно учитывать, что фейковые ресурсы умело маскируются под другие популярные новостные различных агентств, учреждений и организаций. Копируется их дизайн, может меняться в написании URL-адреса всего одна или несколько букв.

2. *Изучите новость целиком*. Не следует судить о новости только по заголовку. С целью привлечения внимания массовой аудитории названия фейковых статей делаются намеренно сенсационными и вызывающими. При внимательном прочтении новости оказывается, что заголовок не соответствует содержанию статьи.

3. *Проверьте автора.* Это реально существующий автор? Можно ли ему доверять? Что о нём пишут в интернете? Если у статьи нет автора, то это часто делается во избежание ответственности.

4. *Есть ли у новости ссылки*. Следует пройти по ссылкам и проверить, действительно ли они поддерживают данную новость? Ссылки приведут к надёжным, авторитетным источникам или к каким-то сомнительным безымянным сайтам? Поддерживается ли эта новость другими источниками интернета?.

5. *Проверьте дату выпуска.* Актуальна ли данная информация? По тексту необходимо проверить также датировку описываемых в статье событий. Часто старые новости перерабатываются и выпускаются как новые, даже если они больше не актуальны.

6. *А может это какая-то шутка?* Некоторые фейковые новости могут быть просто сатирическими заметками, которые умело имитируют стиль и структуру печатной прессы. Просмотрите сайт и информацию об авторе. Возможно, это просто развлекательная, юмористическая статья, созданная для получения комического эффекта.

7. *Оценивайте информацию непредвзято.* Известно, что люди, как правило, склонны больше доверять той информации, которая подтверждает их убеждения, и отрицать ту информацию, которая противоречит их мнению. Следует определиться, влияют ли ваши убеждения на объективное восприятие информации?

8. *Обратитесь к экспертам.* Получите подтверждение специалистов, которые действительно разбираются в данной теме. Кроме того, существуют порталы, которые помогут быстро вычислить фейковую новость, например, FactCheck.org, StopFake.org.

Необходимо знать методы создания фейковой информации, что поможет выявлять ее. Глобальная сеть журналистских расследований (GIJN) характеризует 6 сценариев обмана и пошаговые инструкции по их проверке, выявлению неточностей и фальсификаций:

1. *Манипуляции с изображениями (фотографиями)* – самый простой способ фальсификации новостей, который легко разоблачить. Существует два распространенных способа манипуляции: 1) редактирование изображений в специальных программах, таких как Adobe Photoshop; 2) реальные фото, но сделанные в другое время, в другом месте. В обоих случаях их можно разоблачить, используя обратный поиск изображений в Google (*Google Reverse Search*), меню "Сервис" (опции «Визуально похожие» или «Другие размеры») или TinEye – еще один инструмент обратного поиска, который распознает идентичные или отредактированные копии изображений путем зеркального отражения. Так можно найти обрезанные или смонтированные версии одного и того же фото. Сайт FotoForensics использует метод «анализа уровня ошибок» и помогает найти части изображения, добавленные к нему после редактирования. После обработки фото программа создает изображение с выделенными деталями. Сайты, на которых размещаются фото, также могут предоставить дополнительную информацию об их содержании.

2. *Видео-трюки* – манипуляции происходят также, как и манипуляции с фото, однако разоблачение поддельных видео намного сложнее и более трудоемко. Для создания фейковых новостей с видео чаще всего применяются следующие технологии: использование старых видео для иллюстрации новых событий; помещение видео или его отрывка в другой контекст; создание полностью фальшивого видео, что требует много времени и денег. Злоумышленниками также используется технология *дипфейк (deepfake)*, позволяющая с помощью машинного обучения моделировать поведение и внешность человека на видеозаписи. Методика синтеза изображения, основана на искусственном интеллекте. Она используется для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики. Для создания таких видео используют искусственный интеллект и нейронные сети. Дипфейк (deepfake, подделка) может использоваться для замены определённых элементов изображения на желаемые образы, например, знаменитостей, политиков, поддельных новостей и вредоносных обманов. Такие ролики можно найти на популярных сайтах потокового видео: YouTube, Vimeo, Tik Tok и других.

Для разоблачения фальшивых видео используются многие специализированные интернет-ресурсы: Weather Underground, YouTube DataViewer, InVid, Microsoft Video Authenticator (эти программы

помогут узнать точную дату и время загрузки, проверить, было ли ранее видео размещено в социальных сетях); географические сервисы WikiMapia, Google Maps, Google Street View (для определения места съемки видео) и др.

3. *Перекручивание фактов* – это манипулирование новостями путем использования обманчивых заголовков; мнений, которые представлены как факты, искажения фактов; полностью выдуманные факты; проигнорированные детали; перекручивание цитат или даже придумывание их. Многие люди репостят статьи в социальных сетях после прочтения заголовка, но не читают весь текст. Вводящий в заблуждение заголовок к реальной новости – один из самых распространенных методов создания фейков.

4. *Манипулирование экспертными оценками* – использование псевдоэкспертов или искажение слов реальных экспертов. Псевдоэксперты часто появляются один раз, а потом исчезают. Необходимо проверять подлинность эксперта: посмотреть его биографию, страницы в социальных сетях; сайт той организации, от имени которой он выступает; статьи, комментарии в других медиа и отзывы коллег о его деятельности. Можно обратиться в конкретную организацию. Организации с хорошей репутацией заинтересованы в прекращении распространения дезинформации о них и об их экспертах. То, что представляется как авторитетный аналитический центр, может быть спорным или его вообще может не существовать. В средствах массовой информации в качестве экспертов могут выступать совершенно фейковые лица, которые продвигают определенные политические взгляды или подталкивают аудиторию к определенным решениям (так называемое «изобретение экспертов с нуля»). Часто манипуляторы искажают смысл слов экспертов, вырывая фразы из контекста, подделывают их мнения. Еще одним распространенным методом является манипуляции при переводе слов эксперта с одного языка на другие языки. Следует найти оригинальный материал и перевести его заново.

5. *Манипуляция в масс-медиа.* Может осуществляться путем использования сообщений маргинальных СМИ, блогов с “громкими” именами и ссылающимися на авторитетные медиа. Люди склонны доверять авторитетным СМИ и относиться к ним некритично, что используется пропагандистами и манипуляторами; искажения новостей авторитетных СМИ, указания ссылок на несуществующие сообщения авторитетных СМИ (необходимо перейти на источники по ссылке и оценить их достоверность);

6. *Манипуляции с данными* социологических опросов и экономическими показателями. Это происходит, когда исследования имеют слабую методологию:

− отсутствует глубокая оценка объекта анализа, ситуации, происходит механический подсчет показателей;

− неправильная интерпретация результатов (делается попытка показать результаты правдивыми и достоверными, а в результате искажаются реальные результаты исследований);

− неверные сравнения (часто такие подделки включают в себя некоторые реальные числа с добавлением чисел из подозрительных и ложных источников).

При чтении опросов общественного мнения и других исследований важно обратить внимание на следующее:

− как сформулированы вопросы, не придуманы ли они чтобы манипулировать и навязывать определенные ответы;

− репрезентативна ли выборка респондентов;

− известен ли исследователь в профессиональном сообществе (репутация);

− кто является заказчиком исследования;

− как соотносятся результаты исследования с другими данными и результатами (если они резко отличаются, результаты стоит поставить под сомнение).

Расчет авторов фейковой информации состоит в том, чтобы заманить любопытного читателя на необходимую страницу и перевести его по ссылке на сообщение интригующего характера, текст которого является односторонним или сфабрикованным, а достоверная информация при этом умалчивается. Так и начинается процесс манипуляции сознанием на основе ложных данных.

Информационно-психологическая манипуляция и зомбирование осуществляется посредством насыщения текста сообщений информацией, состоящей из частичной или полной лжи. В результате в сознании читателя неосознанно формируется искажённое восприятие событий и фактов с различной степенью ложности.

Манипуляция основана на подмене истинных причин событий мнимыми, которые дезориентируют объект в нужном для манипулятора направлении. Это один из способов управления большим количеством людей (коллективами, сообществами и так далее) путём создания иллюзий и условий для управления их поведения путем воздействия на психику человека. Манипуляция массовым сознанием служит ключевым элементом *зомбирования и информационной войны*.

Манипуляция приводит к угнетению личности, поскольку человек желает верить в то, что хочет приобрести: знания, материальные блага, опыт, психологический комфорт. Угнетение может достигаться через ложь, в

которую человек хочет верить. Подавляющее большинство людей служат пассивными объектами информационного воздействия (не тратят ни душевных, умственных, физических сил, ни времени, чтобы критически оценить, усомниться в информационных сообщениях), что становится *условием успешной манипуляции.*

Цель манипулятора – дать объектам такие знаки, чтобы в процессе восприятия информации они изменили представление о действительности в желательном для манипулятора направлении и при этом были уверены, что поступают в полном соответствии с собственными желаниями. Манипулятор стремится лишить объекта свободы выбора, способности критически мыслить (а лучше не мыслить вообще) и делать свой рациональный выбор. Он подводит человека к якобы безальтернативной точке зрения по тому или иному вопросу, создает иллюзию и заставляет поверить в нее, что может стать руководством к действию.

Зомбирование – изменение сознания (представлений о реальности) объекта зомбирования без его согласия, путём навязывания заведомо ложной информации с использованием специальных методов для закрепления этой информации в долговременной памяти на уровне представлений о реальности, жизненных убеждений и поведенческих навыков. Для достижения задач манипулирования и зомбирования используются СМИ, социальные сети, специально созданные сайты, а также неформальные каналы информации.

Существует множество методов информационно-психологической манипуляции, некоторые из которых очень созвучны с созданием фейковой информации, но имеют более агрессивный и целеустремленный характер. В известной работе С.Г. Кара-Мурзы «Манипуляция сознанием» приводится 13 таких методов. Приведем их с некоторыми обобщениями:

1. *Использование вербального внушения*. Инициатор манипуляций организуют масштабное «обсуждение» в СМИ продвигаемой им нужной идеи. Излагаются мнения, отобранных им «аналитиков». Отбираются «авторитетные мнения». Зрителя (слушателя, читателя) в прямом смысле «убеждают» принять ту или иную точку зрения «методом вдалбливания в головы», но в более мягкой, нежели традиционная пропаганда, форме.

2. *Намеренное искажение действительности* в СМИ, подача намеренно противоречивой, недостоверной и заведомо предвзятой информации. Может производиться как в грубой форме, так и в завуалированной форме.

3. *Перенос частного факта в сферу общего*, возведение единичного случая в ранг системы. Обратная методика – искусственное дробление единой цепочки событий на отдельные факты.

4. *Использование слухов, домыслов, предвзятых толкований* вместо достоверных фактов и мнений, основанных на анализе имеющейся информации.

5. *Технологии софистического типа,* основанные на приемах подмены понятий, нарушения аргументации, построение дедуктивных и индуктивных цепочек на заведомо неправильных предпосылках (утверждение связи между фактами/ событиями там, где ее в действительности нет). Сюда же относится «подмена событий их словесной декларацией». Под *софизмом* понимается формально кажущееся правильным, но ложное по существу умозаключение. основанное на преднамеренно неправильном подборе исходных положений.

6. *Использование «синдрома приобретенной беспомощности»* – выпячивания в информационном поле негативных новостей и событий (катастрофы, бедствия, войны, эпидемии, разгул преступности), выделение этому большого количества информационного поля (часов эфира, первых полос в газетах). У человека постепенно вырабатывается ощущение, что он живет в «мире зла», вокруг него только болезни, страдания, действуют многочисленные преступники. Это придает ему пассивность и послушание на поведенческом уровне, лишает воли к переменам.

7. *Замалчивание одних фактов и выпячивание других*.

8. *Метод фрагментации* − подача информации кусками, порционно, стремление помешать человеку видеть картину в целом.

9. *Методы, применяемые в классической пропаганде* – многократные повторы, создание эффекта массовости нужной точки зрения, противоположная точка зрения представляется отсталой, непрогрессивной, а ее представители дискредитируются.

10. *Создание ложных авторитетов и экспертов*. Персоналии, транслирующие выгодную манипуляторам точку зрения, незаслуженно возвеличиваются.

11. *Создание лжесобытий, мистификация*. Инициирование заказных информационных поводов.

12. *Подмена фактов и идей* красивыми, но бессодержательными лозунгами, призывами, целями.

13. *Метод диссонанса* – продвижение альтернативных фактов, ценностей и представлений, разрушающих механизмы трансляции исторической памяти, общие символы и ценности.

Важнейшей формой *противодействия* информационно-психологической манипуляции является *критический анализ* информационных сообщений из различных источников, что требует от сотрудников библиотек способностей аналитической обработки информации.

С точки зрения информационной безопасности можно выделить следующие способы противодействия манипуляциям:

– непредвзятый анализ источников информации, в которых представлены различные точки зрения по рассматриваемому вопросу, выявление общих и разнящихся сведений и доведения их до посетителя библиотеки;

– получение информации из первых рук, общение с представителями различных групп, задействованных в проблемной ситуации;

– выявление манипуляторов и анализ продвигаемой ими точки зрения;

– анализ отношения различных групп в социальных сетях и других публичных источниках.

Важным является *умение выявить манипуляторов* и их точки зрения в сети интернет. Чаще всего это происходит путем анализа социальных комментариев. Появление в короткий отрезок времени в разных социальных сетях большого количества однотипных постов, комментариев, и т. п. с элементами нетерпимости, «разжигания конфликта» по рассматриваемой проблеме может свидетельствовать о признаках «манипуляционной атаки».

Эти сообщения могут иметь эмоциональную, экспрессивную окраску, «переход на личности», оскорбления и угрозы. Такие посты часто отличаются «пропагандистскими штампами», а не здравым смыслом. В отношении публичных лиц, неугодных манипуляторам, они могут содержать элементы травли, раскрытия конфиденциальной информации, троллинга, а также содержать массу пустых и провокационных сообщений с целью их дискредитации и нанесения психологической травмы. Все это может подкрепляться множеством публикацией пустых статей, сюжетов, тем, фейковых новостей и обсуждений, чтобы создать у потребителя этого «информационного хаоса» ложного впечатления, что «так думают все». Только постоянный и системный анализ таких информационных сообщений и комментариев позволяет в конце концов распознать специальную заказную акцию и определить ее цель и участников.

Информационные войны являются высшим уровнем реализации информационно-психологических угроз. Существует большое количество определений понятия *«информационная война»*, но чаще всего в двух значениях:

1. Как целенаправленные действия, предпринятые для достижения информационного превосходства путём нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем. Такая трактовка дается в фундаментальных монографиях Г.Г. Почепцова

«Информационные войны» и «Информационные войны: основы военно-коммуникативных исследований».

2. Как процесс противоборства человеческих общностей, направленный на достижение политических, экономических, военных или иных стратегических целей, путём информационного воздействия на гражданское население, власти, вооружённые силы противостоящей стороны. В качестве смежного по значению также используется термин *психологическая война* – психологическое воздействие на гражданское население, военнослужащих другого государства с целью достижения политических или чисто военных целей.

Основной целью информационной войны является изменение сознания, поведения, нравственных установок и здоровья людей, а также информационно-коммуникационных систем противника. В качестве *информационного оружия* для достижения этой цели используются: 1) СМИ, интернет, публичные выступления, беседы, внушение, гипноз и т.п. 2) энергоинформационные системы, воздействующее на психологию и физиологию человека, минуя его сознание (радиолокационные системы, низкочастотные и высокочастотные генераторы, биолокационные установки, химические и биологические средства и др.).

Не осознавая факта воздействия, человек начинает ощущать либо уверенность в себе, либо подавленность, тревогу, страх, агрессивность, зачастую перестает контролировать свои действия. В результате, можно изменить поведение людей, например, снизить или усилить накал демонстраций, беспорядков и этим повлиять на текущие социально-политические процессы.

Задачи применения *информационного оружия*: подрыв международного авторитета государства, его сотрудничества с другими странами; манипулирование общественным сознанием внутри страны, создание атмосферы бездуховности и безнравственности, негативного отношения к национальному наследию; провоцирование политической напряженности и хаоса внутри страны, инициирование этнических и религиозных столкновений, забастовок, массовых беспорядков и других акций протеста; дезинформация населения об истории страны, о работе государственных органов, подрыв их авторитета, дискредитация всей системы управления; нанесение серьезного ущерба жизненно важным интересам государства в политической, экономической, социальной и других сферах деятельности.

Основными *методами* ведения информационных войн, как правило, считаются:

– *вброс дезинформации* противнику, которая понимается в двух аспектах: *как предмет* – заведомо ложная или искажённая информация и *как процесс* – введение в заблуждение путём распространения противнику (конкуренту) неполной или ненужной информации, искажения контекста, искажения части информации для достижения своих целей: деловых, коммерческих, военных;

– представление информации в выгодном для себя ключе.

Данные методы информационно-психологического воздействия позволяют изменять оценку происходящего конкурентами (противником), населением, развивать пораженческие настроения. Цель такого воздействия всегда одна – оппонент должен поступить так, как это необходимо манипулятору.

Обеспечить информационно-психологическую безопасность пользователей библиотеки можно путем решения двух основных задач:

1. Создать в библиотеке *экологическую информационную среду*, комфортные условия, которые бы обеспечивали пользователю возможность свободного доступа и осмысления необходимой информации;

2. Создать постоянно действующую систему формирования *информационной культуры* пользователя библиотеки.

Решение этих двух задач позволит защитить психику посетителя библиотеки, позволит научить его воспринимать полученную информацию не как истину в последней инстанции, а уметь понимать ее суть, интерпретировать ее, уметь находить и анализировать альтернативные точки зрения и на этой основе определять личную позицию.

Тема 6. Политика информационной безопасности библиотеки

Политика информационной безопасности библиотеки – это комплекс мер, правил, процедур и принципов, которыми в своей деятельности руководствуется персонал и пользователи библиотеки, в целях защиты ее информационных ресурсов и объектов информатизации.

Для политики информационной безопасности характерна формализация. Она достигается путем разработки соответствующих документов: положений, регламентов, инструкций, правил. Руководство библиотеки, основываясь на нормативно-правовых и нормативно-технических документах, самостоятельно решает, с помощью каких методов, средств, какая информация и объекты информационной безопасности должны быть защищены.

Важно четко определить: основные критерии эффективности защиты информации; состояние информационной безопасности; обязанности и

ответственность каждого структурного подразделения в системе информационной безопасности библиотеки; права и ответственность пользователей библиотеки.

Разработке и внедрению политики информационной безопасности в библиотеке должна предшествовать оценка ее текущего состояния, что осуществляется с помощью *аудита.*

Аудит информационной безопасности представляет собой целенаправленный процесс получения объективных качественных и количественных оценок об объектах и субъектах информационной безопасности библиотеки по заранее заданным критериям. Аудит позволяет оценить и спрогнозировать риски, управлять их влиянием на все информационные активы библиотеки, обоснованно подойти к созданию или корректировке политики информационной безопасности.

Согласно нормативно-техническим документам (ГОСТам) основными направлениями аудита является:

1. Аттестация объектов информационной безопасности библиотеки, о которых подробно речь шла в теме 2. – библиотечный фонд, базы даных, информационно-коммуникационное оборудование, помещения, технические средства и т.д.

2. Анализ эффективности использования методов и средств для защиты информационных ресурсов библиотеки – выявление каналов утечки информации, способов несанкционированного доступа к ней, эффективности применяемых средств защиты информации;

3. Исследование технических средств библиотеки на наличие побочных электромагнитных излучений – средств связи и обработки информации, локальной компьютерной сети библиотеки и другого в соответствии с требованиями санитарно-гигиенической безопасности;

4. Разработка (уточнение) концепции и политики информационной безопасности библиотеки, т.е. комплекса мер по защите информации.

Различают внешний и внутренний аудит, первичный и плановый. инициативный и обязательный.

Внешний аудит – проводится чаще всего разово и по инициативе руководства библиотеки с приглашением сторонних аудиторских организаций, как правило, на платной основе. В качестве аудиторов выступают независимые эксперты.

Внутренний аудит – осуществляется на непрерывной (плановой) основе в соответствии с требованиями ISO и руководствуется Положением о внутреннем аудите библиотеки. Процесс подготовки и проведения аудита утверждается руководителем библиотеки.

Целями проведения аудита являются:

– анализ угроз и рисков информационной безопасности библиотеки в целом и ее информационным активам;

– оценка текущего состояния защищенности информационных ресурсов АБИС библиотеки и ее информационно-коммуникационной инфраструктуры;

– определение узких мест в системе защиты информации и информационных систем;

– оценка соответствия информационной безопасности библиотеки существующим стандартам и другим нормативно-правовым документам в области информационной безопасности;

– выработка рекомендаций по внедрению новых и совершенствованию существующих механизмов информационной безопасности библиотеки.

В число *дополнительных задач* внутреннего аудита могут входить:

– разработка (корректировка) концепции и политики информационной безопасности библиотеки;

– подготовка распорядительных документов по защите информации с участием аудиторов и их внедрение в практику работы библиотеки;

– постановка задач для руководителей структурных подразделений библиотеки, в первую очередь, связанных с ее автоматизированной системой;

– участие в обучении пользователей и персонала библиотеки вопросам информационной безопасности;

– другие задачи.

Существуют стандартизированные *этапы* проведения аудита информационной безопасности:

1. *Инициирование проведения аудита.* На этом этапе установливаются права и обязанности аудиторов. Это закрепляется в их должностных инструкциях, а также в положении об аудите. Указывается необходимость сотрудникам библиотеки оказывать всяческое содействие аудиторам и представлять им всю необходимую информацию. Разрабатывается и согласовывается с руководством библиотеки план проведения аудита. Издается соответствующий приказ. Определяются границы проведения обследования библиотеки. Все перечисленное обсуждается на рабочем совещании, в котором участвуют аудиторы, руководители библиотеки и ее структурных подразделений;

2. *Сбор информации.* Этот этап является наиболее сложным и длительным, что может быть связано с отсутствием всей необходимой документации и необходимостью постоянного взаимодействия аудиторов со многими руководителями (персоналом) структурных подразделений библиотеки. Для получения достоверных выводов относительно состояния информационной безопасности необходимо наличие всех исходных данных,

документации для анализа, начиная с организационной структуры библиотеки, пользователей ее автоматизированной системы, персонала, обслуживающего ее. На основе представленной организационно-технологической документации определяются требования безопасности к автоматизированной системе и существующие риски во всей ее организационно-функциональной структуре и архитектуре.

3. А*нализ данных аудита.* Существует несколько *методов (подходов)* анализа данных на основе собранной информации:

– *анализ рисков* – самый сложный. Опираясь на методы анализа рисков, рассмотренные ранее, аудиторы определяют индивидуальный набор требований для конкретной обследуемой библиотеки, учитывая ее масштаб и особенности, программно-техническую среду функционирования информационной системы и существующие угрозы безопасности в этой среде;

– *использование профильных стандартов, сертификатов, реестров*, *технических условий* и других нормативно-технических документов информационной безопасности, которые определяют базовый набор требований к основным информационным активам (объектам защиты) библиотеки, а также требованиям системы охраны труда в библиотеке. Аудиторы должны правильно определить набор требований к каждому объекту информационной безопасности библиотеки;

– *использование нормативно-правовых документов* на предмет соответствия им функционирования библиотеки в целом и ее информационно-коммуникационных систем, например, регламентирующих использование интернет, персональных данных, авторских прав и т.д.

– *гибридный подход*, который считается наиболее эффективным и предполагает комбинированное использование предыдущих подходов, когда, например, требования к безопасности автоматизированной системы библиотеки формируются на основе анализа рисков.

4. *Выработка рекомендаций.* Зависит от использованных подходов анализа состояния информационной безопасности библиотеки, степени детализации анализируемых информационных активов при проведении аудита. Но безусловно, рекомендации должны быть конкретными, соответствовать возможностям конкретной библиотеки и быть применимыми, экономически обоснованными и аргументированными, а также представлены по степени важности. Нормативными документами устанавливается, что приоритет должен быть отдан рекомендациям информационной безопасности организационного уровня над программно-техническими методами защиты информации. Однако, от аудиторов не требуется реализация конкретных проектных решений, например, внедрения

программно-технических средств защиты информации. Это требует дальнейшей проработки всех заинтересованных сторон в библиотеке, а аудиторы могут принять в этом деле самое непосредственное участие.

5. *Подготовка аудиторского отчета* является результатом проведения аудита. Качество отчета характеризует эффективность работы аудиторов. Стандартизированный набор требований предполагает, что в нем должны содержаться:

− цели аудита, характеристика обследуемых объектов, границы аудита;

− использованные методы;

− результаты анализа данных аудита;

− обобщающие выводы;

− оценка уровня информационной безопасности библиотеки в целом, а также ее отдельных информационных активов (например, библиотечной компьютерной сети, использования интернет, сохранности фонда и т.п);

− соответствие требованиям нормативно-технических и нормативно-правовых документов;

− рекомендации аудиторов по устранению существующих недостатков и «узких мест»;

− рекомендации по совершенствованию всей системы информационной безопасности в библиотеке.

Как уже отмечалось, данные проведенного аудита служат основой для разработки (совершенствования) концепции информационной безопасности, которая в свою очередь станет основой для разработки политики информационной безопасности библиотеки.

Концепция информационной безопасности библиотеки представляет собой нормативный документ, который системно представляет все основные аспекты ИБ конкретной библиотеки и базируется на действующем законодательстве Республики Беларусь, государственных и международных стандартах, методах и средствах обеспечения ИБ, морально-этических нормах, организационных и финансовых возможностях.

Концепция является методологической основой для проведения в библиотеке единой политики в области обеспечения безопасности ее информационных ресурсов (всех объектов информационной безопасности), а также для принятия управленческих решений и разработки практических мер по ее реализации.

Концепция информационной безопасности библиотеки используется для:

- принятия обоснованных управленческих решений по разработке мер защиты информации;

- выработки комплекса организационно-технических и технологических мероприятий по выявлению и предотвращению угроз информационной безопасности;
- координации деятельности структурных подразделений библиотеки по созданию, развитию и эксплуатации ее автоматизированной системы с учетом требований защиты информации;
- формирования и реализации единой политики в области обеспечения информационной безопасности**.**

Структура и содержание концепции информационной безопасности зависит от типа и вида библиотеки, ее масштабности. Вместе с тем, можно представить следующую примерную структуру концепции:

1. *Общие положения*. В данном разделе приводятся и анализируются:

− основные термины и определения в области информационной безопасности;

− раскрывается правовая основа данного документа;

− основная цель и задачи информационной безопасности библиотеки;

− состояние защищенности ее информационных активов (по результатам проведенного аудита);

− объекты библиотеки, на которые распространяется концепция;

− принципы, положенные в основу построения системы информационной безопасности библиотеки.

2. *Объекты и субъекты информационной безопасности*. Характеризуются:

− степень защиты информационных ресурсов библиотеки;

− защищенность процессов обработки, хранения и передачи информации;

− устойчивость функционирования АБИС и всей информационно-коммуникационной инфраструктуры библиотеки, программно-технических средств;

− эффективность функционирования сайта (портала) библиотеки;

− права доступа к различным объектам информационной безопасности пользователей и персонала библиотеки;

− помещения, в которых размещены «чувствительные» объекты информационной безопасности;

− и другое.

3. *Основные угрозы и риски безопасности.* Характеризуются возможные виды и модели угроз основным объектам и субъектам информационной безопасности библиотеки; модели поведения нарушителей; каналы утечки информации; определяются неправомерные умышленные и неумышленные действия персонала и пользователей библиотеки. Предполагается, что

наивысший уровень эффективности будет тогда, когда для нейтрализации каждой угрозы будет выбрано средство защиты с максимальной эффективностью.

4. *Основные направления обеспечения информационной безопасности.* Описываются методы и средства защиты информационных активов библиотеки: правовые, организационные (административные), физические, технические (программно-аппаратные), морально-этические и др.

5. *Первоочередные мероприятия реализации концепции.* Описываются первоочередные организационные действия, которые необходимо предпринять в ближайшее время и которые обеспечат информационную безопасность. Например: разработать техническое задание по обновлению программно-аппаратного комплекса автоматизированной библиотечно-информационной системы библиотеки; внедрить систему видеонаблюдения; установить сертифицированный межсетевой экран; провести внеплановую техническую диагностику серверов и рабочих станций компьютерной сети библиотеки для определения их возможных уязвимостей; приобрести новые версии антивирусного программного обеспечения и т.п.

Концепция информационной безопасности библиотеки утверждается в установленном порядке и служит документом, определяющим дальнейшие действия организационного характера в области политики информационной безопасности.

Политика информационной безопасности оформляется в виде документированных требований. С практической точки зрения и в соответствии с ГОСТ Р ИСО/МЭК 17799–2005 политику обеспечения информационной безопасности в библиотеке необходимо разбить на несколько уровней: *верхний, средний и нижний*.

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-фильтрация сайтов интернета, использования электронной подписи и т. п. Все документы среднего уровня политики информационной безопасности являются конфиденциальными.

На *нижнем уровне* – разрабатываются 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. (например: правила использования интернет в библиотеке, правила использования электронной почты, правила использования информационных ресурсов, правила противопожарной безопасности) и другие.

Организационную основу реализации политики информационной безопасности библиотеки составляют регламентирующие документы и мероприятия, определяющие:

- организацию режима работы (правила внутреннего распорядка) и охраны библиотеки;
- организацию работы с сотрудниками библиотеки, которая предусматривает: подбор и расстановку персонала; обучение правилам работы с конфиденциальной (служебной) информацией и информационными ресурсами (разработка, использование, учёт, исполнение, возврат, хранение, уничтожение); ознакомление с мерами ответственности за нарушение правил информационной безопасности и защиты информации и др.;
- организацию использования программных и технических средств сбора, обработки, накопления, хранения и размножения информации;
- организацию работы по анализу внутренних и внешних угроз информационным ресурсам библиотеки и выработке мер по обеспечению их защиты;
- организацию систематического контроля за работой персонала и пользователей библиотеки с информационными ресурсами, порядком учёта, архивирования, хранения и уничтожения документов на различных носителях.

В каждом конкретном случае организационные мероприятия носят специфическую для данной библиотеки форму и содержание, направленные на обеспечение безопасности информации в определенных условиях.

3. ПРАКТИЧЕСКИЙ РАЗДЕЛ

3.1 Методические указания к практическим занятиям

Практические занятия представляют особую форму сочетания теории и практики. Их назначение – углубление проработки теоретического материала учебной дисциплины путем регулярной и планомерной самостоятельной работы студентов на протяжении всего срока изучения.

Часть практических занятий проводится на базе библиотек. Их цель – закрепление теоретического материала и формирование практических умений и навыков организации системы информационной безопасности конкретной библиотеки.

При оценке практических занятий особое внимание уделяется активности каждого из студентов в групповых обсуждениях, точности и правильности предложений, ответственности на всех этапах разработки и реализации учебного проекта, связанного с проведением аудита и разработкой концепции информационной безопасности библиотеки.

3.2. Тематика практических занятий

Практическое занятие 1.
Концепция информационной безопасности Республики Беларусь

(2 часа)

Цель занятия – усвоить основные положения базовых документов в сфере информационной безопасности.

Задание и методика выполнения:

I. Студенты самостоятельно изучают «Концепцию информационной безопасности Республики Беларусь» (далее – Концепция) и Закон Республики Беларусь «Об информации, информатизации и защите информации».

II. В результате подготовки необходимо быть готовым ответить на следующие вопросы:

1. В чем состоит значение Концепции и необходимость ее реализации.
2. На чем основывается Концепция.
3. Какие основные понятия и определения используются в Концепции.
4. Как в Концепции определяются понятия: «деструктивное информационное воздействие», «информационная безопасность», «кибербезопасность», «кибертерроризм» и «защита информации».

5. В чем проявляются и как соотносятся между собой гуманитарный и технологический аспекты информационной безопасности.
6. Охарактеризуйте цели и задачи государственной политики в области информационной безопасности.
7. В чем сущность «информационного суверенитета» и «информационного нейтралитета».
8. Охарактеризуйте основные направления безопасности информационного пространства в Республике Беларусь.
9. Какие традиционные устои и ценности рассматриваются в Концепции для противодействия деструктивным информационным воздействиям.
10. Определите сущность безопасности массовой информации.
11. Назовите основные направления обеспечения безопасности информационной инфраструктуры.
12. Как в Концепции трактуется безопасность национального сегмента сети интернет.
13. Почему защита критически важных объектов информатизации (КВОИ) является одной из наиболее важных задач обеспечения национальной безопасности Республики Беларусь.
14. В чем сущность противодействия киберпреступности.
15. Как трактуется в Концепции защита государственной и служебной тайны, информации ограниченного распространения и защита персональных данных.
16. Каковы механизмы реализации Концепции.
17. Как соотносятся между собой «Концепция информационной безопасности Республики Беларусь» и Закон Республики Беларусь «Об информации, информатизации и защите информации», сравните их основные разделы.
18. Сформулируйте место и роль Концепции и Закона в информационной безопасности библиотеки.
19. Какие положения этих документов наиболее применимы к информационной безопасности библиотечно-информационных систем.

III. На заключительной части практического занятия под руководством преподавателя проходит групповое обсуждение основных положений Концепции в соответствии с поставленными выше вопросами, анализируются проблемные моменты, высказываются личные мнения студентов.

Литература:

1. О концепции информационной безопасности Республики

Беларусь [Электронный ресурс]: постановление Совета безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // КонсультантПлюс. Беларусь / ООО «Юрспектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.

2. Об информации, информатизации и защите информации [Электронный ресурс]: Закон Респ. Беларусь, 10 нояб. 2008г., № 455-З: в ред. Законов Респ. Беларусь от 04.01.2014 N 102-З, от 11.05.2016 N 362-З // КонсультантПлюс. Беларусь / ООО «Юрспектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.

Практическое занятие 2.
Анализ рисков информационной безопасности библиотеки

(2 часа)

Цель занятия – овладение методикой выявления и типизации рисков информационной безопасности библиотеки.

Краткие теоретические сведения.

Объект информационной безопасности. Можно выделить четыре основных группы объектов библиотеки, которые могут подвергнуться угрозам информационной безопасности: 1) библиотечный фонд и электронные информационные ресурсы; 2) компьютерно-информационная система; 3) пользователи и работники библиотеки; 4) здание, помещение и оборудование.

Информационный актив – это материальный или нематериальный объект, который является информацией или содержит информацию, служит для обработки, хранения или передачи информации, имеет ценность для организации.

Угроза информационной безопасности – совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности и конфиденциальности информации.

Риск информационной безопасности – это потенциальная уязвимая угроза информационным активам библиотеки, причинение вреда ее пользователям и сотрудникам в следствие возникновения негативного события, связанного с нарушением целостности, конфиденциальности и доступности данных.

Уязвимость – слабость в системе информационной защиты и безопасности в целом, делающая возможной реализацию угрозы.

Задание и методика выполнения:

1. Магистрант загружает в интернете (или использует бумажный вариант) СТБ ISO/IEC 27005-2012 «Информационные технологии. Методы

обеспечения безопасности. Менеджмент рисков информационной безопасности».

2. Знакомится с Приложениями C, D и E ГОСТа.

3. Преподаватель предлагает магистранту (по списку группы) один из объектов (активов) информационной безопасности библиотеки для анализа:

- ✓ Библиотечный фонд
- ✓ Электронные информационные ресурсы (базы данных)
- ✓ Серверы и компьютеры библиотеки
- ✓ Процессы обработки информации в АБИС библиотеки
- ✓ Локальная сеть библиотеки
- ✓ Линии передачи данных и сетевое оборудование
- ✓ Работа в интернет
- ✓ Сайт библиотеки
- ✓ Пользователи библиотеки
- ✓ Персонал библиотеки
- ✓ Здание и помещения библиотеки

4. Магистрант с помощью ГОСТов, а также теоретического материала определяет: тип угрозы, группы угроз, перечень уязвимостей.

5. Затем определяется релевантность для каждого типа/вида угрозы, где D (преднамеренные), A (случайные), E (экологические).

6. Пользуясь одним из методов, представленных в Приложении C ГОСТа магистрант производит оценку рисков объекту информационной безопасности библиотеки.

7. Работа оформляется и сдается на проверку преподавателю в виде таблицы:

Объект ИБ	Тип угрозы	Группы угроз	Перечень возможных уязвимостей	Релевантность	Оценка рисков
1	2	3	4	5	6

8. На последующем занятии происходит взаимное обсуждение представленных результатов.

Литература:

ISO/IEC 27004:2016 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, измерения, анализ и оценка» (Information technology – Security techniques – Information security management – Monitoring, measurement, analysis).

СТБ ISO/IEC 27003-2014 «Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности».

Практическое занятие 3.
Характеристика антивирусных программ для защиты информационных ресурсов библиотеки

(2 часа)

Цель занятия – получение знаний о существующем антивирусном программном обеспечении и особенностях его выбора.

Краткие теоретические сведения. Современный рынок программного обеспечения содержит большое количество пакетов антивирусных программ (утилитов) разного функционального назначения и по разной цене. Их задача – обеспечить максимальную защиту компьютерной сети. Антивирусное программное обеспечение может выполнять разносторонние функции: а) защита от вирусов в реальном времени от всех поступающих угроз; б) обнаружение угроз путем сканирования памяти и содержания жестких дисков компьютеров сети; в) автоматическое обновление используемых антивирусных программ (устаревший антивирус не может обнаруживать новые вирусы и угрозы); г) оповещение о программах, которые пытаются получить доступ к компьютерной сети, среди которых могут быть и вредоносные (блокировка и/или удаление выявленных вирусов), восстановление зараженных информационных объектов; д) контроль безопасности в локальной сети и в Интернете; е) различные дополнительные функции, например, защита входящей и исходящий электронной почты, защита мгновенного обмена сообщениями и чатов, принудительная проверка подключенных к корпоративной сети компьютеров, защита интернет-серфинга (процесса просмотра страниц на веб-ресурсах), ведение протоколов о событиях антивирусной защиты и многие другие. При выборе антивирусного программного обеспечения нужно обращать внимание на наличие перечисленных функций.

Примерный список наиболее популярных антивирусных программ:

- Антивирус Касперского – www.kaspersky.ru;
- Dr. Web – www.drweb.ru;
- Avast! Professional Edition – www.avast.ru;
- Panda Antiviru – www.viruslab.ru;
- Eset NOD32 – www.esetnod32.ru;
- Symantec Norton Anti-Virus – www.symantec.com;
- Trend Micro Internet Security – www.ru.trendmicro.com;
- BitDefender Antivirus – www.bitdefender.com;
- McAfee VirusScan – www.mcafee.com
- Avira AntiVir – www.avira.com/ru

Задание и методика выполнения:

1. Магистрант загружает в интернете демонстрационную версию одного из перечисленных выше антивирусных пакетов и изучает его

функциональные возможности. Собирает из любых доступных источников информацию достоинствах и недостатках данного пакета.

2. Во время посещения одной из республиканских библиотек магистрант анализирует антивирусную базу ее компьютерной системы согласно приведенной таблице:

Название (разработчик, версия)	Объем (Мб)	Возможности защиты и обновления	Возможности оповещения	Контроль безопасности локальной сети	Контроль интернет	Другие функции	Цена
1	2	3	4	5	6	7	8

3. Заполненная таблица с анализом и выводами магистранта сдается преподавателю.

Литература:

СТБ 34.101.8-2006 «Информационные технологии. Методы и средства безопасности. Программные и программно-аппаратные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования».

Практическое занятие 4.
Аудит информационной безопасности библиотеки

(6 часов)

Цель занятия – приобрести навыки учебного аудита информационной безопасности библиотеки и представить его результаты в виде рекомендаций.

Задание и методика выполнения:

Практическая работа выполняется в несколько этапов.

Этап I. Предварительно магистранты изучают предложенные источники по теме практической работы. В аудиторных условиях группа магистрантов под руководством преподавателя определяет основные цели, задачи, содержание и критерии аудита информационной безопасности, а также библиотеки, где будет производиться аудит информационной безопасности;

В качестве основных направлений оценки состояния уровня информационной безопасности в библиотеке можно рекомендовать следующие:

– наличие политики информационной безопасности библиотеки;

– организации информационной безопасности;

– обеспечение информационной безопасности при приеме на работу, во время работы и увольнении сотрудников;

– защищённость информационных ресурсов и информационно-коммуникационных технологий библиотеки;

– безопасность функционирования автоматизированной библиотечно-информационной системы библиотеки;

– информационно-психологическая безопасность посетителей и удаленных пользователей библиотеки;

– физическая безопасность библиотеки;

– управление инцидентами в сфере информационной безопасности;

– соответствие законодательным и нормативным требованиям.

Этап II. Проведение аудита в библиотеке. Последовательность проведения аудита информационной безопасности в библиотеке:

– определение перечня объектов защиты: информационные, программные, физические и пр.

– разработка перечня вопросов для проведения аудита;

– определение документов для анализа в ходе аудита;

– сбор исходных данных;

– анализ собранной информации с определением рисков информационной безопасности, которым подвержена библиотека;

– формирование отчёта и рекомендаций по совершенствованию информационной безопасности библиотеки (сдаются на проверку преподавателю).

Этап III. Выполняется в аудитории. Магистранты выступают с докладами по результатам проведенного аудита, совместно обсуждаются проблемные вопросы. Преподавателем подводятся итоги выполнения работы, уровень ее выполнения.

Литература:

Аверченков В. И. Аудит информационной безопасности. 2-е издание: учеб. пособие для вузов — М.: ФЛИНТА, 2011. — 269 с.

ГОСТ Р ИСО/МЭК 27007-2014 – СМИБ. Руководства по аудиту систем менеджмента информационной безопасности

ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements» (СТБ ISO/IEC 27001-2016 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

3.3 Методические указания к семинарским занятиям

Цель семинарских занятий – проблемное обсуждение предложенных вопросов, базируясь на предварительно изученных по теме семинара источниках и проведенных практических занятиях. Магистрант должен уметь самостоятельно анализировать учебную и научную литературу, делать

сравнительный анализ различных наукометрических баз данных, высказывать свою точку зрения.

Семинарские занятия посвящаются ключевым темам учебной дисциплины. Подготовка к семинару требует изучения основной и дополнительной литературы с целью изложения полных ответов на поставленные вопросы. В ответах обязательно должны приводиться фамилии авторов, подходы и мнения которых отмечаются и анализируются в них.

В процессе семинарских занятий студент должен:

– закрепить знания, полученные на лекциях, в процессе самостоятельной работы;

– организовать самоконтроль по усвоению основных теоретических положений, фактов, понятий, терминов, имен ученых и специалистов;

– развить навыки анализа литературы, участия в дискуссиях, выступлениях с докладами, рефератами, сообщениями.

По итогам семинарского занятия студенту проставляется оценка с учетом его самостоятельных ответов и дополнений по обсуждаемым вопросам.

3.4. Тематика семинарских занятий

Семинар 1.
Информационно-психологическая безопасность библиотек.
(2 часа)

Вопросы для обсуждения:

1. Понятие и основные категории информационно-психологической безопасности (вызовы, угрозы, информационная опасность, информационные войны и др.);
2. Виды вредоносной информации, воздействующей на личность;
3. Защита детей и подростков от информации, причиняющей вред их здоровью и развитию;
4. Методы и средства работы библиотек по предотвращению негативного информационно-психологического воздействия на личность.

Литература:

1. О концепции информационной безопасности Республики Беларусь [Электронный ресурс]: постановление Совета безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // КонсультантПлюс. Беларусь / ООО «Юрспектр», Нац. центр правовой информ. Респ. Беларусь. – Минск,

2019.
2. Агитова, С. Защита детей от ситуаций, угрожающих их жизни, здоровью и развитию / С. Агитова // Народное образование. – 2015. – № 5. – С. 57 – 67.
3. Арутюнов, В. В. Особенности социальных аспектов информационной безопасности / В. В. Арутюнов// Научно-техническая информация. Серия 2. Информационные процессы и системы. - 2018. - № 2. - С. 20-24. - Библиогр.: 9 назв.
4. Астахова Л.В. Библиотека как объект обеспечения информационно-психологической безопасности региона// Весник Кем. ГУКИ, 2012.– № 18.– С. 203 – 207– Режим доступа: https://cyberleninka.ru/article/v/biblioteka-kak-subekt-obespecheniya-informatsionno-psihologicheskoy-bezopasnosti-naseleniya-regiona.
5. Атаманов Г.А. Азбука безопасности. Информационные вызовы, риски и угрозы / Г.А. Атаманов // Защита информации. Инсайд. – 2014. – № 1. – С. 6 - 12.
6. Вылегжанина, Т. Кибербезопасность в библиотеках Украины / Тамара Вылегжанина// Бібліятэчны свет. - 2018. - № 2. - С. 31-32.
7. Грачев, Г.В. Информационно-психологическая безопасность личности. – состояние и возможности психологической защиты / Г.В.Грачев. – СПб.: ПИТЕР, 2004.- 450 с.
8. Леончиков В. Е. Информационно-психологическая безопасность личности: библиотековедческий аспект // Науч. и техн. б-ки. –2008. –№ 12.– С.
9. Михайловская, Снежана. Противопоставить киберугрозам комплексную защиту / Снежана Михайловская// Беларуская думка. –2017. – № 10. – С. 18-25.
10. Солдатова Г. У., Чигарькова С. В., Дренёва А. А., Илюхина С. Н. Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете: Учебно-методическое пособие/ Г. У Солдатова, С. В Чигарькова, А. А. Дренёва., С. Н. Илюхина. – М.: Когито-Центр, 2019. – 176 с. – Режим доступа: file:///C:/Users/Notebook/Desktop/Информационная%20безопасность/my_v_otvete_za_cifrovoy_mir1.pdf.
11. Юшина О. Л. Информационно-психологическая безопасность: библиотековедческий аспект (по материалам зарубежной литературы) // Науч. и техн. б-ки. – 2003. – № 11. – С. 32–45.

Для подготовки к семинару магистранты могут использовать и другие источники, в том числе, сетевые.

Семинар 2.
Политика информационной безопасности библиотеки

(2 часа)

Вопросы для обсуждения:

1. Оценка и управление рисками информационной безопасности в библиотеке.
2. Аудит информационной безопасности.
3. Политика доступа к сетевым службам интернета. Лицензирование.
4. Организация комплексной системы защиты информации в библиотеке.
5. Нормативно-технические и правовые документы. Кадровое обеспечение.

Литература:

1. О концепции информационной безопасности Республики Беларусь [Электронный ресурс]: постановление Совета безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // КонсультантПлюс. Беларусь / ООО «Юрспектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.
2. Об информации, информатизации и защите информации [Электронный ресурс]: Закон Респ. Беларусь, 10 нояб. 2008г., № 455-З: в ред. Законов Респ. Беларусь от 04.01.2014 N 102-З, от 11.05.2016 N 362-З // КонсультантПлюс. Беларусь / ООО «Юрспектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.
3. СТБ ISO/IEC 27005-2012 Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасност ISO/IEC 27004:2016 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, измерения, анализ и оценка» (Information technology – Security techniques – Information security management – Monitoring, measurement, analysis).
4. ГОСТ Р ИСО/МЭК 27007-2014 – СМИБ. Руководства по аудиту систем менеджмента информационной безопасности
5. СТБ ISO/IEC 27003-2014 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности.
6. ISO/IEC 27001:2013 — «Information technology – Security techniques – Information security management systems – Requirements» (СТБ ISO/IEC 27001-2016 Информационные технологии. Методы обеспечения

безопасности. Системы менеджмента информационной безопасности. Требования).

7. Аверченков В. И. Аудит информационной безопасности. 2-е издание: учеб. пособие для вузов — М.: ФЛИНТА, 2011. — 269 с.

8. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002. — 208 с.

9. Карауш А.С. Сервер – под замок, или Как минимизировать риски // Библиотечное дело. – 2007. – № 2. – С. 24 – 27. – Режим доступа: http://www.irbis.tomsk.ru/fulltxt/171651.pdf

Для подготовки к семинару магистранты могут использовать и другие источники, в том числе, сетевые.

4. РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ

4.1. Рекомендации к самостоятельной работе

В целях повышения эффективности усвоения учебного материала по учебной дисциплине и формирования профессиональных компетенций предусматривается самостоятельная работа магистрантов (СРМ), которая направлена на формирование знаний и умений выявлять, анализировать и использовать оригинальные источники информации, в т. ч. на иностранных языках.

Цель самостоятельной работы магистрантов – освоение в необходимом объеме содержания учебной дисциплины через систематизацию, планирование и самоконтроль личной учебной деятельности.

По дисциплине разрабатывается учебно-методический комплекс с материалами и рекомендациями в помощь организации самостоятельной работы магистрантов. В целях оценки качества самостоятельной работы магистрантов осуществляется контроль за ее выполнением.

С учетом цели, задач и содержания дисциплины целесообразно использовать следующие виды самостоятельной работы магистрантов:

− самостоятельный поиск и анализ литературы по темам СРМ;

− составление терминологического словаря и тестов по отдельным темам учебной дисциплины;

– изучение состояния информационной безопасности на базе отдельных библиотек;

– контролируемая самостоятельная работа в виде выполнения индивидуальных заданий в аудитории во время проведения практических занятий под контролем преподавателя;

- подготовка рефератов по индивидуальным темам;

- подготовка к устным опросам, тестам, зачету.

Выполненная работа должна отражать степень усвоения магистрантам основных теоретических вопросов, умение самостоятельно мыслить, обобщать материал, определять проблемы, делать выводы.

4.2 Тематика самостоятельной работы

1. Правовые документы Республики Беларусь в области информационной безопасности.

2. Особенности концепций (доктрин) информационной безопасности в зарубежных странах.

3. Нормативно-технические документы в области информационной безопасности в Республике Беларусь.

4. Использование технологии RFID для защиты библиотечных фондов.

5. Психолого-педагогические аспекты информационной безопасности библиотеки.

6. Деятельность библиотек по защите детей и подростков от информации, причиняющей вред их здоровью и развитию.

7. Морально-этические аспекты информационной безопасности библиотеки.

8. Организационно-административные аспекты информационной безопасности библиотеки.

9. Политика библиотеки в области доступа к сетевым службам интернета.

10. Методика проведения аудита библиотеки.

11. Особенности разработки концепции информационной безопасности библиотеки.

12. Кадровое обеспечение информационной безопасности библиотеки.

4.3. Вопросы к зачету

1. Понятие информационной безопасности и защиты информации.
2. Концепция информационной безопасности Республики Беларусь: общая характеристика.
3. Правовые основы информационной безопасности.
4. Цели, задачи информационной безопасности библиотеки.
5. Объекты информационной безопасности библиотеки.
6. Виды угроз информационной безопасности библиотеки.
7. Формальные методы и средства защиты информации в библиотеке.
8. Неформальные методы и средства защиты информации в библиотеке.
9. Основные понятия и объекты компьютерной безопасности библиотеки.
10. Программно-техническое обеспечение безопасности автоматизированных библиотечно-информационных систем (АБИС) библиотеки.
11. Средства антивирусной защиты серверов и рабочих станций локальных компьютерных сетей библиотеки.
12. Понятие и основные категории информационно-психологической безопасности (вызовы, угрозы, информационная опасность, информационные войны и др.);
13. Виды вредоносной информации, воздействующей на личность;

14. Защита детей и подростков от информации, причиняющей вред их здоровью и развитию;
15. Методы и средства работы библиотек по предотвращению негативного информационно-психологического воздействия на личность.
16. Оценка и управление рисками информационной безопасности в библиотеке.
17. Аудит информационной безопасности.
18. Политика доступа к сетевым службам интернета. Лицензирование.
19. Организация комплексной системы защиты информации в библиотеке.
20. Нормативно-правовые документы в области информационной безопасности библиотеки
21. Политика информационной безопасности библиотеки как совокупность норм, правил, запретов и практических рекомендаций.
22. Кадровое обеспечение информационной безопасности библиотеки.

4.4 Рекомендуемые педагогические технологии и методы преподавания

Для управления учебным процессом и организации контрольно-оценочной деятельности рекомендуется использовать рейтинговую систему оценки учебно-познавательной и исследовательской деятельности магистрантов, вариативные модели управляемой самостоятельной работы.

Для диагностики уровня усвоения знаний и умений рекомендован следующий инструментарий:

– тестовый контроль по дисциплине;

– проверка рефератов по отдельным темам дисциплины;

– устный опрос;

– защита выполненных в рамках управляемой самостоятельной работы индивидуальных (групповых) заданий;

– проведение конференции по одной из проблем с привлечением студентов I ступени обучения;

– зачет, для итоговой диагностики компетенций магистранта по дисциплине.

Оценка учебных достижений магистрантов осуществляется с учетом активности работы на лекционных, лабораторных и практических занятиях, а также по результатам управляемой самостоятельной работы.

4.5 Перечень рекомендуемых средств диагностики результатов учебной деятельности студентов.

В процессе преподавания учебной дисциплины «Информационная безопасность библиотечно-информационных систем» используются следующие методы и технологии обучения:

– проектные технологии;

– технология проблемного обучения;

– коммуникативные технологии, основанные на активных формах и методах обучения (дискуссия, спор-диалог и др.);

– поисково-эвристические методы (анализ документов и нормативных правовых актов, анализ ситуаций);

– методы самостоятельной работы магистрантов (работа с первоисточниками, написание рефератов, подготовка портфолио и др.);

– технология обучения как учебного исследования, которая реализуется на практических занятиях и при самостоятельной работе магистранта;

– контрольно-оценочные методы (ответы на семинарах, тестовые задания).

Рекомендуемые педагогические технологии и методы преподавания направлены на глубокую рефлексию магистрантами материалов учебной дисциплины, стимуляцию их личностного и профессионального развития.

5. ВСПОМОГАТЕЛЬНЫЙ РАЗДЕЛ
5.1 Учебная программа

Учреждение образования
«Белорусский государственный университет культуры и искусств»

УТВЕРЖДАЮ
Проректор по научной работе БГУКИ
_____ В.Р.Языкович

15. 01. 2021 г.
Регистрационный № УД-631/уч.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИБЛИОТЕЧНО-ИНФОРМАЦИОННЫХ СИСТЕМ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности магистратуры
1-23 80 01 Библиотечно-информационная деятельность
Профилизация: Теория и методика научно-исследовательской деятельности

2021

Учебная программа составлена на основе типового учебного плана учреждения высшего образования по специальности II ступени (магистратуры) 1-23 80 01 Библиотечно-информационная деятельность, утвержденного Министерством образования Республики Беларусь, регистрационный № Е 23-2-001/пр/тип. от 23.03.2019.

СОСТАВИТЕЛЬ:
Н.А.Яцевич, заведующий кафедрой библиотечно-информационной деятельности учреждения образования «Белорусский государственный университет культуры и искусств», кандидат педагогических наук, доцент

РЕЦЕНЗЕНТЫ:
Пшибытко М.Г., заведующая научно-исследовательским отделом библиотековедения государственного учреждения «Национальная библиотека Беларуси»
Касап В.А., профессор кафедры информационных ресурсов и коммуникаций учреждения образования «Белорусский государственный университет культуры и искусств», кандидат педагогических наук, доцент

РЕКОМЕНДОВАНО К ИЗДАНИЮ:
Кафедрой библиотечно-иформационной деятельности учреждения образования «Белорусский государственный университет культуры и искусств», протокол № 9 от 24.04.2020 г.);
Президиумом научно-методического совета учреждения образования «Белорусский государственный университет культуры и искусств» (протокол № 1 от 14.10.2020 г.)

Ответственный за редакцию:
Ответственный за выпуск: Н.А.Яцевич

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная дисциплина «Информационная безопасность библиотечно-информационных систем» в учебном плане магистерской подготовки по специальности 1-23 80 01 Библиотечно-информационная деятельность входит в государственный компонент (*модуль «Методология и методика научных исследований”).*

Целью учебной дисциплины является овладение магистрантами знаниями и умениями управления информационной безопасностью в библиотеке в целом, ее библиотечно-информационных технологиях, а также предотвращения потенциальных информационных угроз.

Содержание учебной дисциплины «Информационная безопасность библиотечно-информационных систем» содействует овладению выпускниками магистратуры следующими компетенциями:

– УК-2 Обладать навыками использования современных информационных технологий для решения научно-исследовательских и инновационных задач;

– УПК-3 Уметь выявлять, анализировать и предотвращать потенциальные угрозы целосности, доступности и конфиденциальности информации в библиотечно-информационных системах;

– СК-3 Быть способным осуществлять информационно-аналитическую деятельность, владеть основами управления знаниями, информационного мониторинга и прогнозирования в науке и образовании.

В результате изучения учебной дисциплины магистрант должен

знать:

– терминосистему информационной безопасности;

– нормативно-правовую базу в области информационной безопаности;

– основные виды угроз информационной безопасности библиотеки, способы их обнаружения, предотвращения и устранения;

– основные категории информационно-психологической безопасности при обслуживании пользователей библиотек;

– методы и средства защиты информации в библиотеке;

– организационно-управленческие аспекты создания и поддержки комплексной системы защиты информации в библиотеке.

уметь:

– представлять библиотеку как объект информационной безопасности;

– распознавать основные угрозы целостности и защищенности информационных ресурсов в библиотечно-информационных системах;

– предотвращать угрозы информационно-психологической безопасности пользователей библиотек;

– применять эффективные средства администрирования, повышающие защищенность библиотечно-информационных систем;

владеть:

– формальными и неформальными методами защиты информации в библиотеке;

– методикой осуществления аудита и разработки политики информационной безопасности библиотеки.

В соответствии с учебным планом на изучение учебной дисциплины «Информационная безопасность библиотечно-информационных систем» отводится 94 часа, из которых 52 часа – аудиторные занятия. Примерное распределение учебных часов по видам занятий: лекции – 12 часов, лабораторные занятия – 20 часов, практические занятия – 20 часов. Рекомендуемая форма контроля занятий студентов – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Введение

Цель и задачи учебной дисциплины «Информационная безопасность библиотечно-информационных систем» в магистерской подготовке по специальности 1-23 80 01 Библиотечно-информационная деятельность. Специфика и структура дисциплины. Обзор публикаций и сетевой информации по проблемам информационной безопасности библиотечно-информационных систем. Виды аудиторных занятий. Выполнение практических работ на базе библиотек. Особенности самостоятельной работы. Формы итоговой аттестации.

Тема 1. Информационная безопасность как интегральная научно-практическая проблема

Основные понятия, термины и определения в области информационной безопасности и защиты информации. Виды информационной безопасности. Конфиденциальность, целостность, аутентичность и доступность информации как основные свойства информационной безопасности. Правовые основы информационной безопасности. Национальные и международные нормативно-правовые документы в области информационной безопасности. Основы законодательства Республики Беларусь в области информационной безопасности и защиты информации. Концепция информационной безопасности Республики Беларусь. Особенности концепций (доктрин) информационной безопасности в зарубежных странах.

Тема 2. Библиотека как объект информационной безопасности

«Широкая» и «узкая» трактовка понятия информационной безопасности библиотечно-информационных систем. Цели и задачи информационной безопасности в библиотеке. Система информационной безопасности в библиотеке. Субъекты и объекты информационной безопасности в библиотеке. Библиотечный фонд и электронные информационные ресурсы как основные объекты защиты в библиотеках. Основные виды угроз информационной безопасности библиотеки. Естественные и искусственные угрозы. Угрозы нарушения конфиденциальности информации. Угрозы нарушения целостности

информации. Угрозы нарушения работоспособности системы (отказы в обслуживании).

Тема 3. Методы и средства защиты информации в библиотеке

Комплекс методов и комплекс средств, направленных на предотвращение потерь данных в библиотечно-информационных системах. Формальные (физические, технологические, программные), неформальные (законодательные, административные, организационные, морально-этические) средства защиты информации в библиотеке. Программно-техническое обеспечение безопасности автоматизированных библиотечно-информационных систем (АБИС). Технологические возможности АБИС по обеспечению информационной безопасности библиотеки. Санкционирование доступа различных групп пользователей к АБИС. Использование технологии RFID для защиты библиотечных фондов. Средства антивирусной защиты серверов и рабочих станций локальных компьютерных сетей библиотек.

Тема 4. Информационная безопасность компьютерных систем библиотеки

Основные понятия компьютерной безопасности. Объекты компьютерной безопасности библиотеки: персональные компьютеры, рабочие станции, узлы связи, накопители и хранилища носителей информации, сетевое оборудование, внешние каналы связи. Защита информации от естественных помех при передаче по компьютерным сетям библиотеки. Виды компьютерных вирусов. Защита информации от компьютерных вирусов. Защита информации от несанкционированного доступа. Защита информации от несанкционированных изменений (подмены). Защита информации от сбоев в работе программно-технических средств. Защита библиотечных работников от информационных перегрузок.

Тема 5. Информационно-психологическая безопасность пользователей библиотек

Основные категории информационно-психологической безопасности. Информационные вызовы. Информационные угрозы. Внутренние и внешние информационные угрозы. Источники угроз. Информационная опасность. Фейковая информация. Информационное зомбирование и манипулирование. Информационные войны. Виды вредоносной информации. Средства

информационно-психологического воздействия на личность. Цели, задачи, методы и средства деятельности библиотек по предотвращению негативного информационно-психологического воздействия на личность. Защита детей и подростков от информации, причиняющей вред их здоровью и развитию. Безопасное использование компьютеров и интернета детьми. Информационные болезни. Место и роль формирования информационной культуры в защите от информационных угроз различных групп пользователей библиотек.

Тема 6. Политика информационной безопасности библиотеки

Политика информационной безопасности библиотеки как совокупность норм, правил, запретов и практических рекомендаций. Организация комплексной системы защиты информации в библиотеке. Оценка и управление рисками информационной безопасности библиотеки: определение области защиты, анализ угроз, анализ каналов несанкционированного доступа к информации, анализ комплексной безопасности библиотеки, анализ нарушений режима конфиденциальности, анализ подозрений утраты конфиденциальной информации. Аудит информационной безопасности в библиотеке. Политика доступа к сетевым службам интернета. Лицензирование. Меры административного уровня в политике информационной безопасности библиотеки. Технические нормативные правовые акты в области информационной безопасности. Должностные инструкции по информационной безопасности библиотеки для отдельных категорий сотрудников. Кадровое обеспечение информационной безопасности.

5.2 Учебно-методическая карта учебной дисциплины для дневной формы получения высшего образования

Содержание	Количество аудиторных часов			Количество часов УРС	Форма контроля знаний
	Лекции	Семинарские	Практические		
Введение					
Тема 1. Информационная безопасность как интегральная научно-практическая проблема	2		2	2	тэст
Тема 2. Библиотека как объект информационной безопасности	2		2	2	устный опрос
Тема 3. Методы и средства защиты информации в библиотеке	2			2	презентация
Тема 4. Информационная безопасность компьютерных систем библиотеки	2		2	2	презентация
Тема 5. Информационно-психологическая безопасность пользователей библиотеки	2	2		2	конференция
Тема 6. Политика информационной безопасности библиотеки	2	2	4	4	проект
Всего	12	4	12	14	зачет

5.3 Учебно-методическая карта учебной дисциплины для заочной формы получения высшего образования

Содержание	Количество аудиторных часов		Форма контроля знаний
	Лекции	Семинарские Практические	
Введение			
Тема 1. Информационная безопасность как интегральная научно-практическая проблема	1	2	тэст
Тема 2. Библиотека как объект информационной безопасности	1		устный опрос
Тема 3. Методы и средства защиты информации в библиотеке	1		презентация
Тема 4. Информационная безопасность компьютерных систем библиотеки	2	2	презентация
Тема 5. Информационно-психологическая безопасность пользователей библиотеки	2		презентация
Тема 6. Политика информационной безопасности библиотеки	1	2	проект
Всего	8	6	зачет

5.4 Основная литература

1. Щеглов, А.Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов. - Москва : Юрайт, 2020. - 308, [1] с. : табл., рис. ; 24х16 см. - (Бакалавр и магистр. Академический курс).

2. Алешин, Л.И. Безопасность в библиотеке : учеб.-метод. пособие / Л.И. Алешин.– Москва : Либерея-Бибинформ, 2005. – 248 с. (серия «Библиотекарь и время. XXI век. Вып. 18).

5.5. Дополнительная литература

1. О концепции информационной безопасности Республики Беларусь [Электронный ресурс]: постановление Совета безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // КонсультантПлюс. Беларусь / ООО «Юрспектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.– Режим доступа: http://www.pravo.by/upload/docs/op/P219s0001_1553029200.pdf.– Дата доступа: 24.05.2022.

2. Об информации, информатизации и защите информации [Электронный ресурс]: Закон Респ. Беларусь, 10 нояб. 2008г., № 455-З: в ред. Законов Респ. Беларусь от 04.01.2014 N 102-З, от 11.05.2016 N 362-З // КонсультантПлюс. Беларусь / ООО «Юрспектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019.– Режим доступа: http://www.pravo.by/document/?guid=3871&p0=h10800455.– Дата доступа: 24.05.22.

3. Атаманов, Г.А. Азбука безопасности. Информационные вызовы, риски и угрозы / Г.А. Атаманов // Защита информации. Инсайд. – 2014. – № 1. – С. 6 – 12.

4. ГОСТ Р ИСО/МЭК 15408-1-2002 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200029952. – Дата доступа: 24.05.2022.

5. Грачев, Г.В. Информационно-психологическая безопасность личности. – состояние и возможности психологической защиты / Г.В. Грачев. – Санкт-Петербург : ПИТЕР, 2004. – 450 с.

6. ISO/IEC 27005 Информационная технология – Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности: международный стандарт [Электронный ресурс]. – Режим доступа: https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf. – Дата доступа: 24.05.2022.

7. Перечень стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза [Электронный ресурс]. – Режим доступа: http://www.pravo.by/document/?guid=3871&p0=F01900068. – Дата доступа: 24.05.2022

8. Солдатова, Г.У. Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете : учеб.-метод. пособие [Электронный ресурс] / Г.У. Солдатова, С.В. Чигарькова, А.А. Дренева, С.Н. Илюхина. – Москва : Когито-Центр, 2019. – 176 с. – Режим доступа: http://detionline.com/assets/files/research/my_v_otvete_za_cifrovoy_mir.pdf. – Дата доступа: 24.05.2022.

9. СТБ ISO/IEC 27000-2012 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь» [Электронный ресурс]. – Режим доступа: https://meganorm.ru/Data2/1/4293776/4293776737.pdf. – Дата доступа: 24.05.2022.

10. Andress, J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice / J. Andress. – Syngress, 2014. – 240 p. – ISBN 9780128008126.– Режим доступа: https://books.google.by/books?id=9NI0AwAAQBAJ&pg=PA6&redir_esc=y#v=onepage&q&f=false.– Дата доступа: 24.05.2022.