Лабораторная работа № 1

Тема: Разработка и внедрение политики безопасности организации или учреждения

Цель: приобретение практических навыков разработки и внедрения эффективной политики информационной безопасности организации или учреждения.

Задачи:

1. Научиться выделять и классифицировать особенности информационной или информационно-вычислительной системы (ИВС) конкретной организации или учреждения, как объекта защиты.
2. Овладеть навыками принятия обоснованных решений по организационному и правовому регулированию проблем, относящихся к состоянию безопасности ИВС, обеспечению необходимого уровня защиты информации в ИВС.
3. Овладеть основными приемами анализа угроз информационной безопасности ИВС.
4. Научиться выявлять все возможные угрозы и их источники информационной безопасности в организации или учреждении, анализировать и оценивать собранные данные.
5. Разработать концепцию, основные элементы политики безопасности для организации или учреждения по указанному преподавателем варианту задания.
6. Разработать мероприятия по внедрению предложенной Вами политики безопасности.
7. Результаты выполнения лабораторной работы оформить в виде описания разработанной политики безопасности, а также плана мероприятий по ее реализации.

1.1 Теоретические сведения

1.1.1 Основные понятия из предметной области

*Политика информационной безопасности (ПИБ)*организации или учреждения – совокупность правил, процедур, практических методов, руководящих принципов, *документированных управленческих решений*, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организациииили учреждения в своей деятельности.

Информационная (информационно-вычислительная) система – организационно упорядоченная совокупность документов, технических средств и информационных технологий, реализующая информационные (информационно-вычислительные) процессы.

Информационные процессы – процессы сбора, накопления, хранения,

обработки (переработки), передачи и использования информации.

Информационные ресурсы – отдельные документы или массивы документов в информационных системах.

Объект – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

Субъект – активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

Доступ – специальный тип взаимодействия между объектом и субъектом, в результате которого создается поток информации от одного к другому.

Атака – попытка несанкционированного преодоления защиты системы.

Несанкционированный доступ (НСД) – доступ к информации, устройствам ее хранения и обработки, а также к каналам передачи, реализуемый без ведома (санкции) владельца и нарушающий тем самым установленные правила доступа.

Защита информации — организационные, правовые, программно-технические и иные меры по предотвращению угроз информационной безопасности и устранению их последствий.

Безопасность информации— защищенность информации от нежелательного (длясоответствующих субъектов информационных отношений) ее разглашения (нарушенияконфиденциальности), искажения (нарушения целостности), утраты или снижениястепени доступности информации, а также незаконного ее тиражирования.

Безопасность любого ресурса информационной системы складывается изобеспечения трех его характеристик: конфиденциальности, целостности и доступности,также могут быть включены другие, такие как аутентичность, подотчетность, надежность; или иначе: *информационная безопасность* – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности информации или средств ее обработки:

конфиденциальность(англ.*confidentiality*) компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которымпредоставлены на то соответствующие полномочия;

целостность(англ.*integrity*) компонента предполагает, что он может быть модифицирован толькосубъектом, имеющим для этого соответствующие права; целостность является гарантиейкорректности (неизменности, работоспособности) компонента в любой момент времени;

доступность(англ.*availability*) компонента означает, что имеющий соответствующие полномочиясубъект может в любое время без особых проблем получить доступ к необходимомукомпоненту системы (ресурсу).

1.1.2 Элементы эффективной системы информационной безопасности

Для создания эффективной системы информационной безопасности организации или учреждения целесообразно разработать:

- *концепцию* информационной безопасности, которая определяет в целом цели политики и основные ее принципы в увязке со статусом, целями и задачами организации или учреждения;
- *стандарты* (менеджмента качества) – правила и принципы защиты информации по каждому конкретному направлению деятельности;
- *процедуры* –описание конкретных действий по защите информации при работе с ней: персональных данных, порядка доступа к информационным носителям, системам и ресурсам;
- *инструкции*, содержащие подробное описание (алгоритмы) действий по организации информационной защиты и обеспечения разработанных стандартов и процедур;
- *план мероприятий* по обучению персонала и тестированию знаний сотрудников, имеющих доступ к информационным ресурсам.

Всевышеуказанныеэлементы должны быть взаимосвязанными и не противоречивыми.

Для эффективной организации системы информационной безопасностицелесообразно разработать *аварийные планы*. Они необходимы на случай восстановления информационных систем при возникновении форс-мажорных обстоятельств: аварий, катастроф и т. д.

1.1.3 Концепцияполитики безопасности для организации или учреждения

Концепция политики информационной безопасности (ИБ) разрабатывается в соответствии с законодательством по информационной безопасности Республики Беларусь, соответствующими нормативными документами министерства или ведомства, к которому относится организация или учреждение, а также решениями Оперативно-аналитического центра при Президенте Республики Беларусь (см., например, п. 2.2 в книге [1]).

Обеспечение ИБ на предприятиях и в учреждениях, как правило, является неотъемлемой частью общей системы управления, необходимой для достижения уставных целей и задач. Значимость систематической целенаправленной деятельности по обеспечению ИБ становится тем более высокой, чем выше степень автоматизации бизнес-процессов. Значимость обеспечения ИБ в некоторых случаях может определяться наличием в общей системе информационных потоков предприятия сведений, составляющих не только коммерческую, но и государственную тайну, а также другие виды конфиденциальной информации: сведения, составляющие банковскую тайну, различные виды *персональных данных*, в т.ч. – врачебную тайну, интеллектуальную собственность компаний-партнеров и т.п. Обеспечение ИБ в этой сфере и, в частности, основные требования, организационные правила

и процедуры непосредственно регламентируются указанными в начале данного подраздела документами.

Мероприятия по разработке и внедрению политики информационной безопасности в соответствии со стандартом BS ISO/IEC 27001:2005, на основе которого разработан национальный стандарт России ГОСТ ИСО/МЭК 27001–2006 [2], должны начинаться с определения области действия *системы управления информационной безопасностью*(СУИБ). Определение области действия СУИБ полностью зависит от организации. Областью действия СУИБ может являться вся организация в целом, либо конкретный бизнес-процесс или информационная система.

Решение относительно области действия СУИБ должно учитывать интерфейсы и взаимозависимости этой СУИБ с другими частями организации (находящимися вне области действия СУИБ), другими организациями, поставщиками третьей стороны или любыми другими субъектами, не входящими в СУИБ. Примером является СУИБ, состоящая только из одного конкретного бизнес-процесса. В этом случае другие части организации, которые необходимы СУИБ для повседневного функционирования (например, кадровые ресурсы, финансы, продажи и маркетинг или коммунальные службы), являются интерфейсами и зависимостями, в дополнение к любым другим интерфейсам и зависимостям, которые могут существовать.

ОбластьдействияСУИБдолжнабытьподходящейисоответствоватькаквозможностям организации, такиеответственностизаобеспечениеинформационнойбезопасностивсоответствиистребованиями, определяемымиоценкойрисковиприменимымизаконодательнымииинормативнымимеханизмамиконтроля. Длятого, чтобы заявитьобэтомсоответствии, изобластидействияСУИБнедолжнобытьисключеноничего, чтоказываетвлияниенаспособностьи/илиответственностьорганизациизаобеспечениеинформационнойбезопасностивсоответствиистребованиями, определяемымиоценкойрисковисоответствующиминормативнымитребованиями.

*Примерная структура концепции информационной безопасности***.**Основными разделами концепции могут быть следующие:

- определение ИБ (или СУИБ);
- структура информационной системы организации (учреждения) и вытекающая из этого *структура системы обеспечения информационной безопасности*;
- безопасность информации: принципы и стандарты;
- оценка рисков информационным ресурсам в организации (учреждении);
- описание основных механизмов контроля безопасности;
- обязанности и ответственность каждого отдела, управления или департамента, каждого сотрудника в реализации разработанной и утвержденной политики безопасности;

- обязанности лица (администратора безопасности), ответственного за организацию оперативного контроля и управления политикой безопасности;
- ссылки на документы о информационной безопасности, действующие на территории РБ.

Помимо упомянутых выше законодательных и нормативных актов, в общем плане структура системы обеспечения ИБ должна базироваться на *организационно-технических и режимных мерах и методах***.** Для построения политики ИБ рассматривают следующие направления защиты ИВС:

- защита объектов ИВС;
- защита процессов, процедур и программ обработки информации;
- защита каналов связи;
- подавление побочных электромагнитных излучений;
- управление системой защиты.

Организационная защита обеспечивает:

- организацию охраны, режима, работу с кадрами и с документами;
- использование технических средств безопасности (например, простейших дверных замков, магнитных или иных карт и др.), информационно-аналитическую деятельность по выявлению внутренних и внешних угроз.

Оперативно-аналитический центр при Президенте РБ требует, например, от государственных организаций и учреждений выполнения следующих «рекомендаций по обеспечению безопасности информации в локальных сетях, подключенных к сети Интернет» [3]:

- осуществлять предоставление доступа сотрудникам органа (организации) к сервисам сети Интернет (электронная почта, передача файлов, информационные ресурсы и др.) в соответствии с определенным в государственном органе порядком;
- определить правила работы сотрудников с сервисами сети Интернет (электронная почта, передача файлов, доступ к информационным ресурсам, IP-телефонии, социальным сетям и публичным системам мгновенных сообщений);
- определить администраторов сети, их права и обязанности;
- определить права и обязанности пользователей;
- определить ответственность сотрудников и должностных лиц за обеспечение защиты информации;
- обеспечить контроль использования сотрудниками в глобальных сетях: IP-телефонии, социальных сетей и публичных систем мгновенных сообщений;
- определить порядок и перечень используемого программного обеспечения на средствах вычислительной техники сотрудников;
- определить порядок применения средств защиты информации, установленных в локальной вычислительной сети;
- определить необходимые мероприятия по разграничению доступа к средствам защиты информации и обработки информации;
- определить регламент смены атрибутов безопасности (паролей) пользователей;
- определить порядок действий при возникновении нештатной ситуации (сбои, повреждения и отказы) с информационными ресурсами;
- определить регламенты резервирования и уничтожения информации;

- определить порядок контроля, учета использования ресурсов сети Интернет пользователями, формирования и предоставления руководству организации отчетных документов.

Перечисленные требования можно рассматривать как элементы (процедуры и инструкции) рассмотренной в п. 1.2 *эффективной системы ИБ*.

При этом использование технических, программно-аппаратных и программных средств должно:

- обеспечить межсетевое экранирование с использованием собственных возможностей и (или) возможностей уполномоченных поставщиков интернет-услуг;
- обеспечить идентификацию абонентских устройств в локальной сети;
- обеспечить блокирование неконтролируемого обмена информацией между рабочими местами пользователей в локальной сети;
- исключить использование на рабочих местах в локальной сети постороннего программного обеспечения, ресурсов сети Интернет, предназначенных для сокрытия действий пользователя;
- исключить подключение рабочего места в локальной сети к сетям связи общего пользования через другие каналы доступа (сотовый телефон, модем);
- обеспечить синхронизацию системного времени от единого (общего) источника (в качестве источника использовать службу единого времени Белорусского государственного института метрологии);
- осуществлять сбор и хранение данных авторизации и статистики использования сети Интернет пользователями в течение 1 года;
- обеспечить возможность анализа использования сети Интернет пользователями (с использованием собственных возможностей или поставщиков интернет-услуг);
- применять криптографические протоколы для защиты данных авторизации при работе с сервисами сети Интернет.

Британский стандарт BS 7799-3:2006 – Руководство по менеджменту рисков ИБ(специалисты часто ссылаются на него при изучении и анализе вопросов разработки политики безопасности; его перевод можно найти в [4]) – рекомендует в основу концепции политики ИБ положить:

- идентификацию (описание) ресурсов;
- идентификациютребованийзаконодательстваибизнеса, применимыхкидентифицированнымресурсам;
- оцениваниеидентифицированныхресурсовсучетомидентифицированныхтребований законодательстваибизнеса, атакжепоследствийнарушения конфиденциальности, целостностиидоступности.

1.1.4 Оценка рисков информационным ресурсам

Общая характеристика факторов, влияющих на безопасность ИВС

Фактор, воздействующий на ИВС, – это явление, действие или процесс, результатом которых может быть утечка, искажение, уничтожение данных, блокировка доступа к ним, повреждение или уничтожение системы защиты.

Все многообразие дестабилизирующих факторов можно разделить на два класса: внутренние и внешние.

Внутренние дестабилизирующие факторы, влияющие:

1) на программные средства (ПС):

- некорректный исходный алгоритм;

- неправильно запрограммированный исходный алгоритм (первичные ошибки);

2) на аппаратные средства (АС):

- системные ошибки при постановке задачи проектирования;
- отклонения от технологии изготовления комплектующих изделий и АС в целом;
- нарушение режима эксплуатации, вызванное внутренним состоянием АС.

Внешние дестабилизирующие факторы, влияющие:

1) на программные средства:
   - неквалифицированные пользователи;
   - несанкционированный доступ к ПС с целью модификации кода;
2) на аппаратные средства:
   - внешние климатические условия;
   - электромагнитные и ионизирующие помехи;
   - перебои в электроснабжении;
   - недостаточная квалификация обслуживающего персонала.

Риски и их оценка.

В соответствии с [2,4]оценкарисковвключаетвсебяследующиедействияимероприятия:

- идентификациязначимыхугрозиуязвимостейдляидентифицированны хресурсов.
- оценкавероятностивозникновенияугрозиуязвимостей.
- вычислениерисков;

оцениваниерисковпозаранееопределеннойшкалериска.

Все многообразие потенциальных угроз безопасности информации по природе ихвозникновения разделяются на два класса: *естественные* (объективные) и *искусственные*(субъективные).

Естественные угрозы— это угрозы, вызванные воздействиями на информационнуюсистему и ее компоненты объективных физических процессов техногенного характера илистихийных природных явлений, независящих от человека.

Искусственные угрозы— это угрозы, вызванные деятельностью человека. Срединих, исходя из мотивации действий, можно выделить:

- *непреднамеренные* (неумышленные, случайные) угрозы, вызванные ошибками впроектировании информационной системы и ее элементов, ошибками в действияхперсонала и т.п.;
- *преднамеренные* (умышленные) угрозы, связанные с корыстными, идейными илиными устремлениями людей (злоумышленников).

Источники угроз по отношению к самой информационной системе могут быть как*внешними*, так и *внутренними*(о чем мы вспоминали выше).

Основные источники угроз безопасности информации можно классифицировать как:

непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей)нарушения установленных регламентов сбора, обработки и передачи информации, а такжетребований безопасности информации и другие действия пользователей ИВС (в том числе сотрудников, отвечающих за обслуживание и администрированиекомпонентов корпоративной информационной системы), приводящие кнепроизводительным затратам времени и ресурсов, разглашению сведений ограниченногораспространения, потере ценной информации или нарушению работоспособностикомпонентовИВС;

преднамеренные (в корыстных целях, по принуждению третьими лицами, со злымумыслом и т.п.) действия легально допущенных к информационным ресурсампользователей (в том числе сотрудников, отвечающих за обслуживание иадминистрирование компонентов корпоративной информационной системы), которыеприводят к непроизводительным затратам времени и ресурсов, разглашению сведенийограниченного распространения, потере ценной информации или нарушениюработоспособности компонентов информационной системы:

- *деятельность преступных групп и формирований*, политических и экономическихструктур, разведок иностранных государств, а также отдельных лиц по добываниюинформации, навязыванию ложной информации, нарушению работоспособности ИВС в целом и ее отдельных компонентов;
- *удаленное несанкционированное вмешательство посторонних лиц*изтерриториально удаленных сегментов корпоративной информационной системы ивнешних информационно-телекоммуникационных сетей общего пользования (преждевсего, сеть Интернет) через легальные и несанкционированные каналы подключения ктаким сетям, используя недостатки протоколов обмена, средств защиты и разграничениядаленного доступа к ресурсам;

ошибки, допущенные при разработке компонентов информационной системы и системыеезащиты, ошибки в программном обеспечении, отказы и сбои технических средств(в том числе – средств защиты информации и контроля эффективности защиты).

В заключение целесообразно отдельно отметить «человеческий фактор»,классифицировавфизическихлиц,которые могут получить (а часто и реализуют)несанкционированный доступ к информации. К ним следует отнести:

сотрудников организации (учреждения):

- программисты, системные администраторы и даже администраторы информационной безопасности,
- технический персонал;

лиц, не являющихся сотрудниками:

- посетители офиса,
- ранее уволенные сотрудники (особенно «обиженные» увольнением),

- хакеры.

С учетом изложенного *основные факторы (угрозы)*ресурсамможно идентифицировать следующим образом:

1) действия внутреннего или внешнего злоумышленника (несанкционированный, в том числе – удаленный – доступ с целью нарушения работоспособности ИВС, кражи, удаления или модификации информации, несанкционированного распространение материальных носителей за пределами организации);

2) наблюдение за источниками информации;

3) подслушивание конфиденциальных разговоров и акустических сигналов работающих механизмов;

4) перехват электрических, магнитных и электромагнитных полей, электрических сигналов и радиоактивных излучений;

5) разглашение информации компетентными людьми;

6) утеря носителей информации;

7) несанкционированное распространение информации через поля и электрические сигналы, случайно возникшие в аппаратуре;

8) воздействие стихийных сил (наводнения, пожары и т. п.);

9) сбои и отказы в аппаратуре сбора, обработки и передачи информации;

10) отказы системы электроснабжения;

11) воздействие мощных электромагнитных и электрических помех (промышленных и природных).

Несанкционированный доступ с помощью *деструктивных программных средств* осуществляется, как правило, через компьютерные сети.

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и ее ресурсов. На основе таких данных могут быть выбраны необходимые средства управления ИБ.

При оценивании рисков учитывается:

• ценность ресурсов;

• оценка значимости угроз;

• эффективность существующих и планируемых средств защиты.

Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами:

• количественными (например, стоимостными);

• качественными (могут быть построены на использовании таких понятий, как, умеренный или чрезвычайно опасный);

• их комбинацией.

Рассмотрим пример создания шкалы для численной оценки рисков от несанкционированного доступа (НСД) к информационным ресурсам банка [1] (таблица 1.1).

Таблица 1.1 — Условная численная шкаладля оценки ущерба банку от НСД

Величинаущерба	Описание

0	Раскрытие информации принесет ничтожный моральный и финансовый ущерб банку (фирме)
1	Ущерб от атаки есть, но он незначителен, основные финансовыеоперации и положение банка на рынке не затронуты
2	Финансовые операции не ведутся в течение некоторого времени,за это время банк терпит убытки, но его положение на рынке и количество клиентов изменяются минимально
3	Значительные потери на рынке и в прибыли. От банка уходит ощутимая часть клиентов
4	Потери очень значительны, банк на период до года теряет положение на рынке. Для восстановления положения требуются крупныефинансовые займы
5	Банк прекращает существование

Можно конкретизировать определение вероятности наступления угрозы ресурсу. Вероятность того, что угроза реализуется, можно определитьна основе следующих факторов:

• привлекательность ресурса как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;

• возможность использования ресурса для получения дохода как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;

• технические возможности угрозы, используемые при умышленном воздействии со стороны человека;

• вероятность того, что угроза реализуется;

• степень легкости, с которой уязвимость может быть использована.

Вопрос о том, как провести границу между допустимыми и недопустимыми рисками, решается пользователем. Очевидно, что разработка политики безопасности требует учета специфики конкретных организаций.

Пример создания шкалы вероятности того, что угроза будет реализована, приведен в таблице 1.2.

Таблица 1.2 — Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

Вероятность события	Средняя частота события (НСД)
0	Данный вид атаки отсутствует
0,1	Реже, чем раз в год
0,2	Около 1 раза в год
0,3	Около 1 раза в месяц
0,4	Около 1 раза в неделю
0,5	Практически ежедневно

Далее можно создать таблицу рисков (таблица 3). На этапе анализатаблицы риски задаются некоторым максимально допустимым уровнем (порогом), например, значением 0,5.

Далее проверяется каждая строка таблицы: превышен или непревышен порог для значения риска, связанного с анализируемойатакой? Если такое

превышение имеет место, данная атака должнарассматриваться с точки зрения одной из первоочередных целейразработки политики безопасности (таблица 1.3).

Таблица 1.3 — Оценка рисков

Описание атаки	Ущерб	Вероятность	Риск (Ущерб * Вероятность)
Спам (переполнение почтовогоящика)	1	0,4	0,4
Копирование жесткого диска изцентрального офиса	3	0,1	0,3
…	…	…	…
Итого			

Если интегральный риск (итого) превышает допустимый уровень, значит, в системе безопасности набирается множество мелких проблем, которые также нужно решать комплексно. В этомслучае из строк таблицы (типов атак) выбираются те, которые«дают» самый значительный вклад в значение интегрального риска. Производится работа по снижению их влияния или полномуустранению.

1.1.5 Мероприятия по внедрению политики безопасности

После того, как документация по информационной безопасности готова, необходима плановая деятельность по ее внедрению в повседневную работу.Основу таких мероприятий, как было указано в плане выполнения лабораторной работы, составляют *инструкции*, содержащие подробное описание (алгоритмы) действий по организации информационной защиты и обеспечению разработанных стандартов и процедур, и *план мероприятий* по обучению персонала и тестированию знаний сотрудников, имеющих доступ к информационным ресурсам.

Можно выделить следующие общие направления мероприятий:

• управление персоналом;

• физическая защита инфраструктуры ИВС;

• поддержание работоспособности ИВС;

• реагирование на нарушения режима безопасности ИВС;

• планирование восстановительных работ.

Управление персоналом заключается в выполнении следующих условий. Во-первых, для каждой должности существовать квалификационные требования по ИБ. Во-вторых, в должностные инструкции должны входить разделы, касающиеся информационной безопасности. В-третьих, каждого работника нужно научить мерам безопасности теоретически и на практике.

Меры физической защиты включают в себя защиту от утечки информации по техническим каналам, инженерные способы защиты и т.д.

Планирование восстановительных работ предполагает:

• слаженность действий персонала во время и после аварии;

• наличие заранее подготовленных резервных производственных площадок;

• официально утвержденную схему переноса на резервные площадки основных информационных ресурсов;

• схему возвращения к нормальному режиму работы.

Поддержание работоспособности включает в себя создание инфраструктуры, включающий в себя как технические, так и процедурные регуляторы и способной обеспечить любой наперед заданный уровень работоспособности на всем протяжении жизненного цикла информационной системы.

Реагирование на нарушение режима безопасности может быть регламентировано в рамках отдельно взятой организации. В настоящее время, осуществляется только мониторинг компьютерных преступлений в национальном масштабе и на мировом уровне.

Основой программно-технического уровня являются следующие механизмы безопасности:

• идентификация и аутентификация пользователей;

• управление доступом;

• протоколирование и аудит;

• криптография;

• экранирование;

• обеспечение высокой доступности и т.д.

Таким образом, политика информационной безопасности должна рассматриваться как *система*, как комплекс инструментов по защите информации.

1.2 Практическое задание

Разработать политику информационной безопасности организации согласно варианту, представленному в таблице 1.4, а также план мероприятий по ее реализации.

Отчет по лабораторной работе оформить в соответствии с СТП БГТУ 001-2010.

Придерживайтесь следующей структуры отчета.

*Титульный*лист(см. приложение 1)**.**

1. *Обоснование* актуальности, цели и задачи разработки ПИБ в организации (учреждении) .

2. *Объектызащиты***.** Описание структуры организации (учреждения), периметра и внутренней структуры ИВС. Полный обзор всех возможных объектов, а также субъектов информационных отношений, для защиты которых должны быть приняты меры по обеспечению информационной безопасности.

3. *Основные угрозы и их источники.*Анализ потенциальных угроз: естественных и искусственных, а также преднамеренных и непреднамеренных, внешних и внутренних.

4. *Оценка угроз, рисков и уязвимостей.*Анализ ценности ресурсов, оценка значимости угроз, а также эффективности существующих и планируемых средств защиты (воспользуйтесь приведенными в описании таблицами, заполните их).

5. *Меры, методы и средства обеспечения требуемого уровня защищенностиинформационныхресурсов.*Описаниеразработаннойполитики ИБ и программы обеспечения безопасности на всех уровнях работы организации (учреждения).

Выводы и предложения.

Таблица 1.4 — Варианты для разработки политики безопасности

Вариант	Тип организации или учреждения
1	Учебная организация. Школа
2	Event-компании
3	Консалтинговая компания
4	Поликлиника
5	Издательство
6	Юридическая компания
7	Страховая компания
8	Банк
9	Туристическая компания
10	Логистическая компания
11	Учебная организация. Университет
12	Интернет-магазин
13	Маркетинговая компания
14	Оператор мобильной связи
15	ИТ-компания
16	Больница
17	Библиотека

1.3 Вопросы для контроля и самоконтроля

1. Охарактеризовать актуальность и основные причины проблемы информационной безопасности организации, страны.
2. Сформулировать цели и задачи политики информационной безопасности.
3. Охарактеризовать основные угрозы информационной безопасности каждой организации (учреждения) из таблицы 4.
4. Как правильно проводить оценку рисков?
5. Что должна включать в себя программа внедрения политики информационной безопасности?

Лабораторная работа № 2

Тема: Элементы теории информации. Параметры и характеристики дискретных информационных систем

Цель: приобретение практических навыков расчета и анализа параметров и информативных характеристик дискретных ИС

Задачи:

1. Закрепить теоретические знания по основам теории информации.
2. Разработать приложение для расчета и анализа параметров и информативных характеристик дискретных ИС.
3. Результаты выполнения лабораторной работы оформить в виде описанияразработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

2.1 Теоретические сведения

2.1.1 Основные понятия из предметной области

Передача информации (данных) осуществляется между двумя абонентами, называемыми *источником сообщения* (ИсС) и *получателем сообщения* (ПС). Третьим элементом информационной системы является *канал* (среда) *передачи*, связывающий ИсС и ПС.

Отметим также, что и в системах с хранением информации всегда можно выделить ИсС и ПС. В данном случае каналом передачи здесь выступает устройство хранения информации (память). Например, при записи данных в ОЗУ (оперативное запоминающее устройство) компьютера в качестве ИсС и ПС может выступать процессор (соответственно при записи и чтении данных).

Таким образом, простейшая информационная система состоит из трех элементов: источника сообщения, канала передачи сообщения и получателя сообщения.

Отображение сообщения обеспечивается изменением какой-либо физической величины, характеризующей процесс (например, амплитуда, частота, фаза). Эта величина является *информационным параметром сигнала*(в общем случае – информационной системы).

Сигналы, как и сообщения, могут быть *непрерывными* и *дискретными*. Информационный параметр непрерывного сигнала с течением времени может принимать любые мгновенные значения в определенных пределах. Непрерывный сигнал часто называют *аналоговым,* а каналы и устройства функционирующие на основе такого типа сигналов – аналоговыми..

Дискретный сигнал(устройство или канал передачи) характеризуется конечным числом значений информационного параметра.

Дискретные сообщения состоят из последовательности *дискретных знаков*. Часто этот параметр принимает всего два значения (0 или 1).

Сообщение или канал его передачи на основе этих двух значений сигнала называют *двоичным* или *бинарным*.

Построение сигнала по определенным правилам,обеспечивающим соответствие между сообщением и сигналом, называют *кодированием*.

Кодирование в широком смысле– *преобразование сообщения в сигнал*.

Кодирование в узком смысле – *представление исходных знаков*, называемых символами, в другом алфавите с меньшим числом знаков. Оно осуществляется с целью повышения надежности и преобразования сигналов к виду, удобному для передачи по каналам связи. Последний тип кодирования относится к так называемой *прикладной теории кодирования информации*, занимающейся поиском и реализацией методов и средств обнаружения несоответствий (*ошибок*) между переданным X_k и принятым Y_kсообщениями.

2.1.2 Основные характеристики и параметры двоичных систем

Рассмотрим основные характеристики и параметры двоичных систем.

Важнейшая характеристика источника, получателя или канала – алфавит.

*Алфавит,**A***– это общее число знаков или символов (N), используемых генерации или передачи сообщений. Символы алфавита будем обозначать через $\{a_i\}$, где $1 \le i \le N$; N – *мощность алфавита*.

Минимальное число элементов алфавита $N_{\min}=2$, $\boldsymbol{A}=\{0,1\}$ – двоичный код. Один дискретный знак представляет собой *элементарное сообщение*, последовательность знаков – сообщение.

Набор элементов алфавита, создаваемых дискретным источником сообщений, заранее, априори (до опыта) известен получателю.ИСс в каждый дискретный момент времени выдает один элемент алфавита. Этот элемент сообщения является одним из символов алфавита. Понятно, что ПС заранее не известно, какой это элемент. Если обозначить вероятность выбора каждого элемента алфавита $p(a_i)$, то

$$\sum_{i=1}^{N} p(a_i) = 1.$$

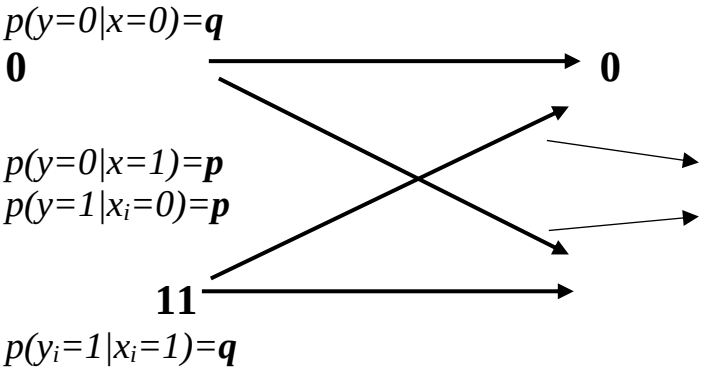
Вероятности $p(a_i)$могут быть получены в результате анализа частотных свойств символов алфавита, если на входе такого анализатора принять документ на основе соответствующего алфавита. Причем объем документа должен быть таким, чтобы от частости (частоты) появления каждого символа в анализируемом документе можно было перейти к вероятности соответствующего события.Можно предположить, что указанному требованию будет объем электронного документа *не менее нескольких десятков килобайт*.

*Двоичный канал передачи информации*строится на основе двоичного алфавита:$\boldsymbol{A}=\{0,1\}$.При этом канал, в котором вероятности искажения

переданного 0 (принята соответственно 1; этому событию соответствует *условная вероятностьр(1|0)*) и переданной 1 (принят соответственно 0; этому событию соответствует условная вероятность*р(0|1),*) равны, как и равны вероятности передачи 0 (*р(0)*)и 1 (*р(1)*), называют *двоичным симметричным каналом (ДСК)*.

В общем случае, если передается сообщение $X_k=x_1, x_2, \ldots, x_k$,а принимается сообщение $Y_k= y_1, y_2, \ldots, y_k$, то рассмотренные условные вероятности можно рассматривать с двух точек зрения: $p(x_i|y_j)$и$p(y_j|x_i)$.

На рисунке 2.1 схематично представлен ДСК.



ИСо (отправитель) ПС (получатель)

Рисунок 1.1 -Схематичное представление двоичного симметричного канала

На рисунке 1.1 обозначены: *q*– вероятность правильной (безошибочной) передачи бита сообщения, *p*– вероятность передачи бита с ошибкой. Понятно, что $p + q = 1$.

Информационной характеристикой алфавита (источника сообщений на основе этого алфавита) является *энтропия*.

Этот термин применительно к техническим системам был введен Шенноном и Хартли.

Энтропию алфавита $\boldsymbol{A}=\{a_i\}$ по К.Шеннону рассчитывают по следующей формуле:

$$\mathrm{H}_S(A) = -\sum_{i=1}^{N} P(a_i) * \log_2 P(a_i), \qquad (2.1)$$

С физической точки зрения *энтропияалфавитапоказывает, какое количество информации приходится в среднем на один символ алфавита*.

Частным случаем энтропии Шеннона является энтропия Хартли. Дополнительным условием при этом является то,что все вероятности одинаковы и постоянны для всех символов алфавита. С учетом этого формулу (2.1) можно преобразовать к виду:

$$H_{Ch}(A) = \log_2 N. \qquad (2.2)$$

Сообщение X_k, которое состоит из k символов, должно характеризоваться определенным *количеством информации*, $I(X_k)$:

$$I(X_k) = H(A) * k. \quad (2.3)$$

Здесь$H(A)$– энтропия алфавита с соответствующим распределением вероятностей $p(a_i)$.

Если принять, что $p(a_i = 1) = p(1)$ и $p(a_i = 0) = p(0)$, используя (2.1), вычислим энтропию бинарного алфавита:

$$H(A_2) = -p(0)*\log_2(p(0)) - p(1)*\log_2(p(1)). \quad (2.4)$$

К примеру, полагая что сообщение X_k состоит только из единиц (X_k= =11…1) и имеет длину k, т.е. вероятность того, что произвольный символ равен единице, составляет единицу ($p(a_i = 1)$=1), и другая вероятность –- $p(a_i = 0)$=0 для $i = \overline{1, N}$. Фактически, здесь имеет место использование *моноалфавита*: алфавита, состоящего из одного символа.

Учитывая, что сумма $)p(1) + p(0)$==1 и, выразить одну вероятность через другую (например, $p(1) = 1-p(0)$), можно теоретически доказать информативность бинарного алфавита, решив дифференциальное уравнение $[dH(A)/dp(1)] = 0$ (вспомним из курса математики, как найти экстремум функции; можно для этого воспользоваться [5]).

Если вероятность ошибки в ДСК отлична от 0 ($p > 0$), переданное сообщение может содержать ошибки: $X_k \neq Y_k$. Количество информации в таком сообщении при его передаче по ДСК будет определять не энтропией двоичного алфавита (в соответствии с (2.3)), а эффективной энтропией $H_e(A)$ алфавита или пропускной способностью канала:

$$H_e(A) = 1 – H(Y|X), \quad (2.5)$$

где $H(Y|X)$ – условная энтропия и

$$H(Y|X) = –p \log_2 p – q \log_2 q. \quad (2.6)$$

2.3 Практическое задание

1 Создать приложение для расчета и анализа параметров и информативных характеристик дискретных ИС, с помощью которого:

а) рассчитать энтропию указанного преподавателем алфавитов: один – на латинице, другой – на кириллице(по формуле (2.1) – перейти от частоты появления каждого символа алфавита к соответствующей вероятности); в качестве входного может быть принят произвольный электронный текстовый документ на основе соответствующего алфавита; частоты появления символов

алфавитов оформить в виде гистограмм (можно воспользоваться приложением MSExcel);

б) для входных документов, представленных в бинарных кодах, определить энтропию бинарного алфавита;

в) используя значения энтропии алфавитов, полученных в пп. а) и б), подсчитать количество информации в сообщении, состоящем из собственных фамилии, имени о отчества (на основе исходного алфавита – а) и в кодах ASCII–б); объяснить полученный результат;

г) выполнить задание п. в) при условии, что вероятность ошибочной передачи единичного бита сообщения составляет: 0.1; 0.5; 1.0.

2.3 Вопросы для контроля и самоконтроля

1. Что такое «алфавит источника сообщения»?
2. Что такое «мощность алфавита источника сообщения»?
3. Какова мощность алфавита белорусского языка?
4. Какова мощность алфавита русского языка?
5. Какова мощность алфавита «компьютерного» языка?
6. Что такое «энтропия алфавита»?
7. Что такое «энтропия сообщения»?
8. От чего зависит энтропия алфавита?
9. Записать формулу для вычисления энтропии.
10. Что нужно знать для вычисления энтропии алфавита?
11. Как рассчитываются энтропия Шеннона и энтропия Хартли? В чем принципиальное различие между этими характеристиками? Дайте толкование физического смысла энтропии.
12. Поясните назначение знака «минус» в формулах (2.1) и (2.4).
13. Что такое избыточность алфавита и избыточность сообщений, сформированных в компьютерных системах? Принцип действия каких систем основан на существовании данной избыточности?
14. Расположите в порядке возрастания энтропии известные вам алфавиты.
15. Вычислить энтропию алфавита белорусского (русского) языка.
16. Вычислить энтропию Шеннона бинарного алфавита, если вероятность появления в произвольном документе на основе этого алфавита одного из символов составляет 0.25, другого – 0.75; либо 0 и 1.0; либо 0.5 и 0.5.
17. Чему равна энтропия алфавита по Хартли, если мощность этого алфавита равна: а) 1 символ, б) 2 символа, в) 8 символов?