**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 организации или 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 (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

**Безопасность любого ресурса информационной системы складывается из обеспечения 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), которым предоставлены на то соответствующие полномочия; **целостность** (англ. integrity) компонента предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права; целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени; **доступность** (англ. availability) компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту 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 обеспечению разработанных стандартов и процедур;  
• план мероприятий по обучению персонала и тестированию знаний сотрудников, имеющих доступ к информационным ресурсам.

Все вышеуказанные элементы должны быть взаимосвязанными и непротиворечивыми. Для эффективной организации системы информационной безопасности целесообразно разработать аварийные планы. Они необходимы на случай восстановления информационных систем при возникновении форс-мажорных обстоятельств: аварий, катастроф и т. д.

**1.1.3. Концепция политики 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. 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 том числе врачебная тайна, интеллектуальная 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 Р 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 бизнеспроцесс 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 бизнеспроцесса. 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.

Область действия СУИБ должна быть подходящей и соответствовать как возможностям организации, так и ее ответственности за обеспечение информационной безопасности в соответствии с требованиями, определяемыми оценкой рисков и применимыми законодательными и нормативными механизмами контроля. Для того чтобы заявить об этом соответствии, из области действия СУИБ не должно быть исключено ничего, что оказывает влияние на способность и/или ответственность организации за обеспечение информационной безопасности в соответствии с требованиями, определяемыми оценкой рисков, и соответствующими нормативными требованиями.

Основными разделами *концепции информационной* безопасности 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 об информационной безопасности, действующие на территории Республики Беларусь.   
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 Республики Беларусь требует, например, от государственных организаций и учреждений выполнения следующих «рекомендаций по обеспечению безопасности информации в локальных сетях, подключенных к сети Интернет»:   
• 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;   
• определять правила работы сотрудников с сервисами сети Интернет (электронная почта, передача файлов, доступ к информационным ресурсам, IP-телефонии, социальным сетям и публичным системам мгновенных сообщений);   
• определять администраторов сети, их права и обязанности;   
• определять права и обязанности пользователей;   
• определять ответственность сотрудников и должностных лиц за обеспечение защиты информации;   
• обеспечивать контроль использования сотрудниками в глобальных сетях: IP-телефонии, социальных сетей и публичных систем мгновенных сообщений;   
• определять порядок и перечень используемого программного обеспечения на средствах вычислительной техники сотрудников;   
• определять порядок применения средств защиты информации, установленных в локальной вычислительной сети;   
• определять необходимые мероприятия по разграничению доступа к средствам защиты информации и обработки информации;  
• определять регламент смены атрибутов безопасности (паролей) пользователей;   
• определять порядок действий при возникновении нештатной ситуации (сбои, повреждения и отказы) с информационными ресурсами;   
• определять регламенты резервирования и уничтожения информации;   
• определять порядок контроля, учета использования ресурсов сети Интернет пользователями, формирования и предоставления руководству организации отчетных документов.

Перечисленные требования можно рассматривать как элементы (процедуры и инструкции) эффективной системы ИБ. При этом использование технических, программно-аппаратных и программных средств должно обеспечивать:   
• межсетевое экранирование с использованием собственных возможностей и (или) возможностей уполномоченных поставщиков Интернет-услуг;   
• идентификацию абонентских устройств в локальной сети;   
• блокирование неконтролируемого обмена информацией между рабочими местами пользователей в локальной сети;   
• исключение использования на рабочих местах в локальной сети постороннего программного обеспечения, ресурсов сети Интернет, предназначенных для сокрытия действий пользователя;   
• невозможность подключения рабочего места в локальной сети к сетям связи общего пользования через другие каналы доступа (сотовый телефон, модем);   
• синхронизацию системного времени от единого (общего) источника (в качестве источника использовать службу единого времени Белорусского государственного института метрологии);   
• осуществление сбора и хранения данных авторизации и статистики использования сети Интернет пользователями в течение 1 года;   
• возможность анализа использования сети Интернет пользователями (с использованием собственных возможностей или поставщиков Интернет-услуг);   
• применение криптографических протоколов для защиты данных авторизации при работе с сервисами сети Интернет.

Британский стандарт BS 7799-3:2006 «Руководство по управлению рисками информационной безопасности» (специалисты часто ссылаются на него при изучении и анализе вопросов разработки политики безопасности; его перевод можно найти в источнике [4]) рекомендует в основу концепции политики ИБ положить:   
• идентификацию (описание) ресурсов;   
• идентификацию требований законодательства и бизнеса, применимых к идентифицированным ресурсам;   
• оценивание идентифицированных ресурсов с учетом идентифицированных требований законодательства и бизнеса, а также последствий нарушения конфиденциальности, целостности и доступности.

**1.1.4. Оценка рисков для информационных ресурсов**

**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 влияют: 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 влияют:   
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] оценка рисков включает в себя следующие действия и мероприятия:   
• идентификация значимых угроз и уязвимостей для идентифицированных ресурсов;   
• оценка вероятности возникновения угроз и уязвимостей;   
• вычисление рисков; оценивание рисков по заранее определенной шкале риска.

Все многообразие потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные). **Естественные угрозы** – это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека.

**Искусственные угрозы** – это угрозы, вызванные деятельностью человека.

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 следующим образом:**

• непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей ИВС (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов ИВС;

• преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т. п.) действия легально допущенных к информационным ресурсам пользователей (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы:   
− деятельность преступных групп и формирований, политических и экономических структур, разведок иностранных государств, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности ИВС в целом и ее отдельных компонентов;   
− удаленное несанкционированное вмешательство посторонних лиц из территориально удаленных сегментов корпоративной информационной системы и внешних информационно-телекоммуникационных сетей общего пользования (прежде всего сеть Интернет) через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам;

• ошибки, допущенные при разработке компонентов информационной системы и системы ее защиты, 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», классифицировав физических лиц, которые могут получить (а часто и реализуют) несанкционированный доступ к информации. К ним следует отнести:

1) сотрудников организации (учреждения):   
• программисты, системные администраторы и даже администраторы информационной безопасности;   
• технический персонал;   
2) лиц, не являющихся сотрудниками: • посетители офиса; • ранее уволенные сотрудники (особенно «обиженные» увольнением); • хакеры.

С учетом изложенного основные факторы (угрозы) ресурсам можно 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 распространения 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).

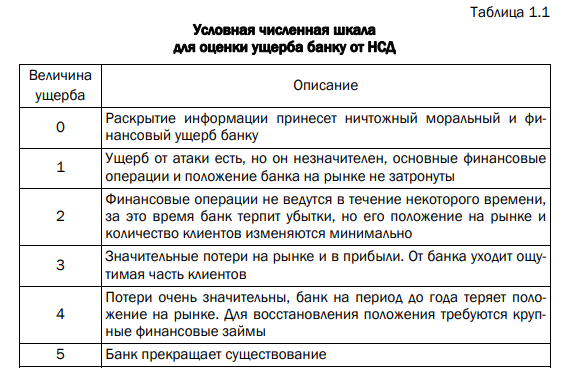
Несанкционированный доступ с помощью деструктивных программных средств осуществляется, как правило, через компьютерные сети.

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 учитываются:

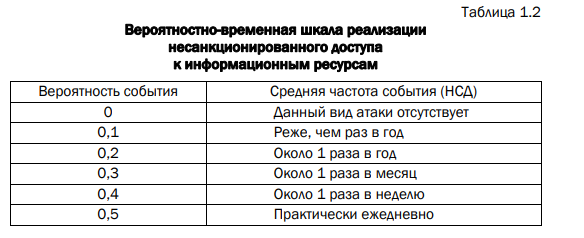
• ценность ресурсов;   
• оценка значимости угроз;   
• эффективность существующих и планируемых средств защиты. Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами:   
• количественными (например, стоимостными);   
• качественными (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] (табл. 1.1).



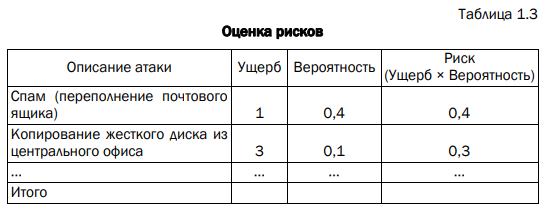
Можно конкретизировать определение вероятности наступления угрозы ресурсу. Вероятность того, что угроза реализуется, определяется на основе следующих факторов:

• 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 табл. 1.2. Таблица 1.2



Далее можно создать таблицу рисков (табл. 1.3). На этапе анализа таблицы риски задаются некоторым максимально допустимым уровнем (порогом), например значением 0,5.

Далее проверяется каждая строка таблицы: превышен или не превышен порог для значения риска, связанного с анализируемой атакой? Если такое превышение имеет место, данная атака должна рассматриваться с точки зрения одной из первоочередных целей разработки политики безопасности (табл. 1.3).



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

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

2. Объекты защиты. 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 защищенности информационных ресурсов. Описание разработанной политики ИБ и программы обеспечения безопасности на всех уровнях работы организации (учреждения). Выводы и предложения.