Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Электронная тетрадь по дисциплине

«Защита информации и надежность информационных систем»

Студент: Самосейко Д.А.

ФИТ 3 курс 2 группа

Преподаватель: Берников В.О.

Вариант: 10

Минск 2021

**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.

* 1. **Теоретические сведения**
  2. **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 организации и 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. **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.

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

* 1. **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., 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 логистическую 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, должны начинаться с определения области *действия системы управления информационной безопасности* (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.

Область действия СУИБ должна быть подходящей и соответствовать как возможностям организации, такие и 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.

*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»:

* 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;
* 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. **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).

1. 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.

1. на аппаратные средства:

* внешние климатические условия;
* электромагнитные и ионизирующие помехи;
* перебои в электроснабжении;
* недостаточная квалификация обслуживающего персонала.
  1. **Риски и их оценка**.

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. Среди них, исходя из мотивации действий, можно выделить:

* *непреднамеренные* (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п.;
* *преднамеренные* (умышленные) угрозы, связанные с корыстными, идейными или иными 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 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 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:

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)* 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 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.

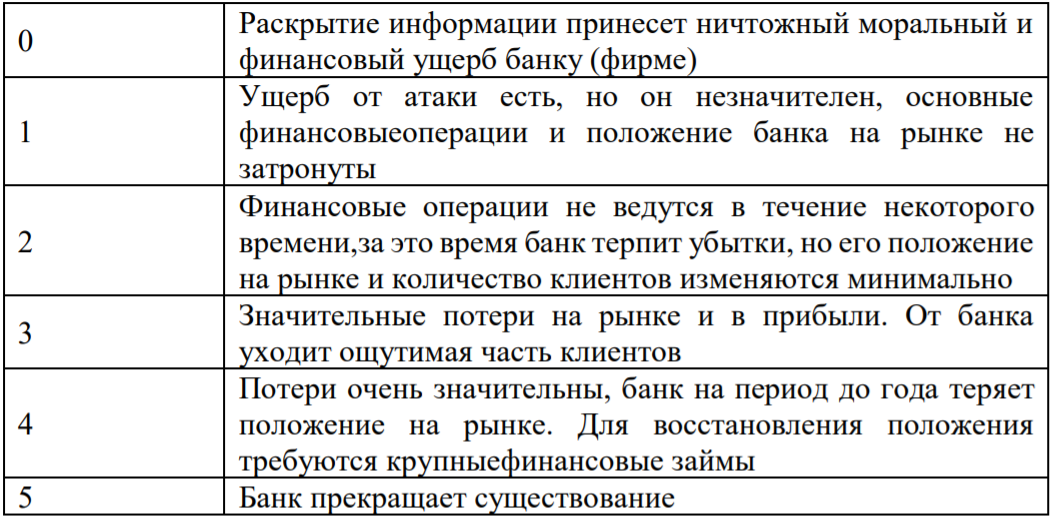
При оценивании рисков учитывается:

1. ценность ресурсов;
2. оценка значимости угроз;
3. эффективность существующих и планируемых средств защиты.
4. 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 компании(таблица 1.1).

Таблица 1.1 — Условная численная шкала для оценки ущерба компании от НСД



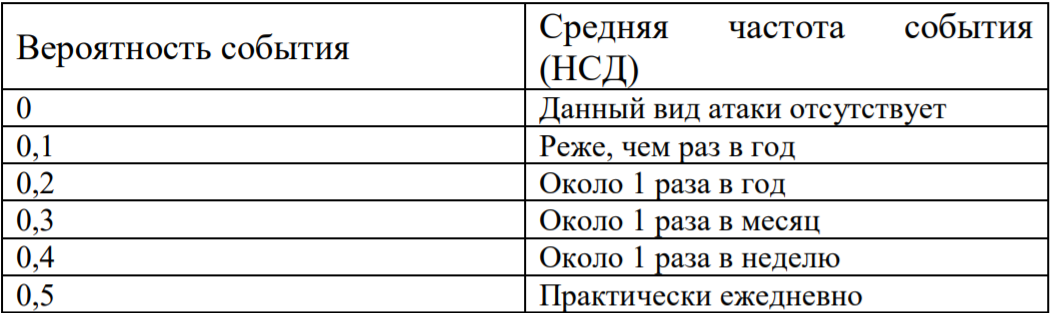
Можно конкретизировать определение вероятности наступления угрозы ресурсу. Вероятность того, что угроза реализуется, можно определить на основе следующих факторов:

* 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 таблице 1.2.

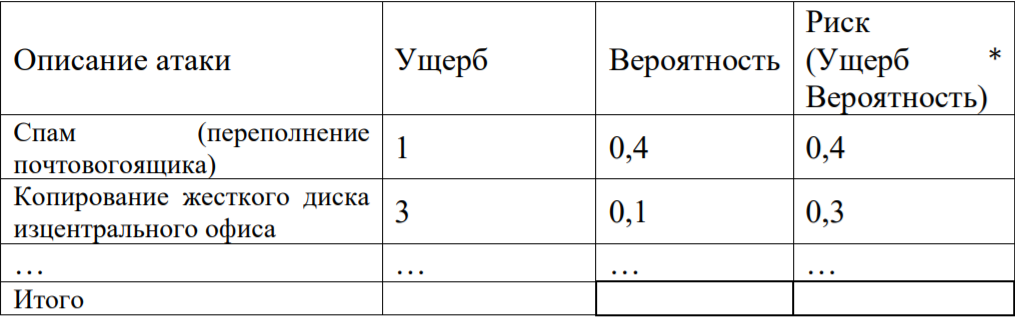
Таблица 1.2 — Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам.



Далее можно создать таблицу рисков (таблица 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 (таблица 1.3).

Таблица 1.3 — Оценка рисков



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 значительный вклад в значение интегрального риска. Производится работа по снижению их влияния или полному устранению.

* 1. **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. **Практическое задание**

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

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.

Все вышеуказанные элементы должны быть взаимосвязанными и не противоречивыми. Для эффективной организации системы информационной безопасности целесообразно разработать *аварийные планы*.

Они необходимы на случай восстановления информационных систем при возникновении форсмажорных обстоятельств: аварий, катастроф и т. д.



*Рисунок 1. Схема структуры ПИБ*

1. *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.

Объект защиты – логистическая компания.



*Рисунок 2 – Структура Логистической компании*

**Организационная структура логистической компании** – внутренняя организация работы транспортного учреждения, с помощью которой структурируются и формализуются подходы и методы управления, определяются группы исполнителей, разрабатываются системы контроля и внутриорганизационных взаимоотношений.

Упрощенно внутреннюю систему логистической компании можно представить так:

* Высшее руководство логистической компании – собрание учредителей, директор.

Это уже элемент текущего, оперативного управления. В его подчинении находятся руководители всех прочих подразделений.

Здесь обычно выделяют:

* **Бухгалтерия.** Структура обязательная для любого хозяйствующего субъекта, и всегда имеющая единое руководство.
* **Управление операций на фондовом рынке.** В распоряжении логистических компаний, на разных условиях, оказываются ценные бумаги многих предприятий и государств. Для обращения с этими активами логистические компании могут формировать специальные службы.
* **Юридическое управление.** Существует во всех логистических компаний, имеет в своем названии указание на специализацию и единое руководство.
* **Управление развития.** Сюда относятся элементы системы связанные с поиском новых рынков, клиентов, направлений и способов дохода. Отделы развития создаются при разных управлениях или объединяются в единую службу при тесном взаимодействии с другими подразделениями.
* **Пиар (PR) и реклама.** Эти направления могут выделяться в отдельные логистические структуры, могут объединяться с управлением развития, или подчиняться подразделениям, ориентированным на определенных клиентов.
* **Управление информационных технологий.** По мере компьютеризации систем обработки информации и развитием удаленного управления, подобные службы стали обязательной частью любой логистической структуры. Они взаимодействуют со всеми отделами, но обычно составляют единую систему.
* **Региональные подразделения.** Такие элементы присущи крупным компаниям. Система управления в них варьируется по нескольким критериям. Иногда региональные подразделения дублируют в своем составе все перечисленные выше управления и службы, иногда курируют только некоторые направления, к примеру – работу с физическими лицами.
* **Отраслевые управления.** Создаются не всегда, но могут быть необходимы лог-компаниям, имеющим особые интересы в определенных отраслях или массового потребителя в одной сфере деятельности: сельском хозяйстве, международной торговле, энергетике и др.

1. *Основные угрозы и их источники. Анализ потенциальных угроз:*

*естественных и искусственных, а также преднамеренных и непреднамеренных, внешних и внутренних.*

**Классификация потенциальных угроз безопасности логистических компаний:**

* Первая группа - физические угрозы.
* Вторая группа - технические угрозы.
* Третья группа - интеллектуальные угрозы.

Физические угрозы, как воздействие физических лиц, совершающих противоправные действия методом физического насилия, также и природные, техногенные катастрофы.

**К физическим угрозам относятся:**

* похищения и угрозы похищения сотрудников компании, членов их семей и близких родственников;
* убийства, сопровождаемые насилием, издевательствами и пытками;
* разбойные нападения с целью завладения денежными средствами, ценностями и документами;
* уничтожение собственности компании и собственности работников;
* угроза безопасность компании;
* террористические акции, т.е. совершение преступления в форме взрыва, поджога, применения или угрозы применения взрывных устройств, химических, биологических, токсических ядов, веществ, а также захват заложников, транспортных средств и т.д.;
* чрезвычайные обстоятельства - это события вызванные аварией и приведшее на определенной территории к угрозе жизни и здоровью людей, ущербу государственным, коммерческим и иным видам собственности, личного имущества граждан и природной среде.

**Технические угрозы** - это совокупность мероприятий и технических средств, направленных на получение нужной информации, а также на нарушение, нейтрализацию аппаратных средств и программного обеспечения интересующего объекта, к ним относятся:

* перехват информации;
* радиоразведка связи и управления;
* искажение информации;
* ввод ложной информации;
* информационное нападение;
* уничтожение информации и т. д.

Цель - перехватить, исказить, уничтожить информацию

**Интеллектуальные угрозы** - это угрозы направленные на продукт интеллектуального труда, умственные способности индивида.

* «Беловоротничковые угрозы (преступления)»;
* "Золотые воротнички";
* Мошенничество;
* Преступления с использованием пластиковых платежных средств:
* операции с поддельными картами;
* операции с украденными/поддельными картами;
* многократная оплата услуг и товаров;
* мошенничество с почтовыми/телефонными заказами ;
* многократное снятие со счета;
* мошенничество с использованием подложных слипов;
* использование для выдачи наличных денег через банкомат;

1. *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).

Таблица 1 — Условная численная шкала для оценки ущерба издательства от НСД.

*Таблица 1*

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб компании |
| 1 | Ущерб от атаки есть, но он незначителен, основные финансовые операции и положение компании на рынке не затронуты. |
| 2 | Финансовые операции не ведутся в течении некоторого времени, за это время компания терпит убытки, но его положение на рынке и количество клиентов изменяются минимально. |
| 3 | Значительные потери на рынке и в прибыли. От компании уходит ощутимая часть клиентов. |
| 4 | Потери очень значительны, компания на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы. |
| 5 | Компания прекращает существование |

Можно конкретизировать определение вероятности наступления угрозы ресурсу. Вероятность того, что угроза реализуется, можно определить 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.

Таблица 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 анализа таблицы риски задаются некоторым максимально допустимым уровнем (порогом), например, значением 0,5.

Таблица 3 — Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (Ущерб \* Вероятность) |
| разглашение информации компетентными людьми | 3 | 0.3 | 0.9 |
| подслушивание конфиденциальных разговоров и акустических сигналов работающих механизмов | 3 | 0.3 | 0.9 |
| наблюдение за источниками информации | 2 | 0.3 | 0.6 |
| отказы системы электроснабжения | 5 | 0.1 | 0.5 |
| воздействие мощных электромагнитных и электрических помех (промышленных и природных) | 2 | 0.2 | 0.4 |
| Итого | 13 | 1.2 | 3.2 |

1. *Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Описание разработанной политики ИБ и программы обеспечения безопасности на всех уровнях работы организации (учреждения).*

Меры безопасности:

Учитывая возможные виды угрозы/атаки, можем выделить следующие рекомендации, либо советы, следуя которым возможно снизить риски опасного воздействия и их последствий:

* обеспечение безопасности функционирования компании его кредитно-финансовой деятельности и защиты конфиденциальной информации;
* организация работы по правовой, организационной и инженерно-технической защите материальных, финансовых и информационных ресурсов;
* организация специального делопроизводства, исключающего несанкционированного получения конфиденциальных сведений;
* выявление и локализация возможных каналов разглашения, утечки и несанкционированного доступа к конфиденциальной информации в процессе повседневной деятельности и в экстремальных ситуациях;
* обеспечение режима безопасности при проведении всех видов деятельности, включая встречи, переговоры, совещания, связанные с деловым сотрудничеством на национальном и международном уровнях;
* обеспечение охраны зданий, помещений, оборудования и технических средств обеспечения деятельности компании;
* обеспечение безопасности персонала;
* информационно-аналитическая деятельность в интересах оценки ситуации и выявления неправомерных действий злоумышленников и конкурентов.
* обеспечение режима безопасности при проведении всех видов деятельности, включая встречи, переговоры, совещания, связанные с деловым сотрудничеством на национальном и международном уровнях;
* обеспечение охраны зданий, помещений, оборудования и технических средств обеспечения деятельности компании;
* обеспечение безопасности персонала;
* информационно-аналитическая деятельность в интересах оценки ситуации и выявления неправомерных действий злоумышленников и конкурентов.

**Дополнения и вывод.**

Так же, эффективной мерой по защите является проведение тестовых экспериментов по атаке на фирму: наем специализированных людей, которые проведут атаку на сетевые ресурсы компании и выявят пробелы в защите. Данная операция безусловно является дорогостоящей, однако впоследствии, это сэкономит средства компании.

**Вывод:** важно помнить, что, прежде чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Этапы построения политики безопасности — это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности. При этом политику безопасности желательно оформить в виде отдельного документа и утвердить руководством предприятия.