Содержание детализированной политики безопасности

Рассмотрим основное содержание разделов ПБ по отдельным направлениям защиты информации.

Организация внутриобъектового режима и охраны помещений и территорий является частью общей работы предприятия по обеспечению сохранности имущества и непрерывности текущей деятельности.

Основной задачей обеспечения внутриобъектового режима является недопущение посторонних лиц к информационным активам и предотвращение угроз информационной безопасности.

Основой внутриобъектового режима является пропускной режим, в рамках которого, как правило, устанавливаются:

- документы, дающие право прохода на территорию предприятия – как пропуска и карты доступа, выданные самим предприятием, так и документы, выданные сторонними организациями (например, служебные удостоверения должностных лиц некоторых органов государственной власти);
- категории пропусков, используемых на предприятии, в соответствии с которыми (категориями) ограничивается срок действия пропусков, время возможного прохода на территорию предприятия (дни недели, часы суток) и некоторые другие параметры;
- порядок выдачи, обмена, продления и изъятия пропусков, а также порядок действий сотрудников и должностных лиц при утрате пропуска;

- порядок организации пропуска лиц, автотранспорта и проноса (провоза) имущества: размещение и порядок работы контрольно-пропускных пунктов, возможность пропуска тех или иных лиц, средств автотранспорта и грузов через те или иные КПП и др.;
- основные положения документооборота, используемого при проходе посетителей на территорию предприятия — требования к ведению Журнала регистрации прохода посетителей, требования к документам, на основе которых выдаются разовые пропуска, порядок выдачи разовых пропусков и т.п.;
- порядок досмотра транспортных средств, допускаемых на территорию предприятия.

Кроме того, в рамках организации внутриобъектового режима может быть предусмотрено разделение помещений и территорий на отдельные зоны с ограничением доступа (в том числе на основе разделения помещений и территорий на различные категории), а также разграничение доступа отдельных сотрудников (категорий персонала) и посетителей в различные зоны; также могут быть определены основные требования к техническим средствам разграничения доступа и организации их использования.

С технической точки зрения меры по обеспечению пропускного и внутриобъектового режимов могут быть реализованы теми же средствами, которые используются для обеспечения безопасности в других сферах, помимо информационной (защита имущества и персонала, обеспечение непрерывности производственного процесса), – средствами контроля доступа, видеонаблюдения, сигнализации и физической защиты.

В основе средств контроля доступа лежат механизмы опознавания личности и сравнения с установленными параметрами. Политика предприятия может устанавливать как упрощенные подходы к опознаванию, когда охранники предприятия проверяют документы (подтверждение личности, подтверждение возможности прохода на территорию в данное время через данный КПП), так и использование автоматизированных средств, когда опознание посетителя и подтверждение (либо запрет) возможности прохода на территорию (выхода с территории, из здания) производится автоматизированной системой контроля доступа на основе имеющихся у посетителя машиночитаемых средств персональной идентификации (пластиковых карт, жетонов и т.п.)

либо на основе считывания и анализа его физических особенностей (геометрии лица, отпечатков пальцев, рисунка радужной оболочки глаза, голоса и т.п.).

При выборе конкретных средств биометрической идентификации специалистам и руководителям предприятия следует помнить, что разные технологии имеют разную степень надежности, а также могут быть более или менее удобными в повседневном использовании большим количеством людей.

Так, например, считается, что одна из передовых технологий биометрической идентификации – идентификация по кровеносным сосудам пальца (когда инфракрасный луч просвечивает палец и создает трехмерное изображение уникальной для каждого человека структуры кровеносных сосудов) – существенно менее уязвима для обмана, чем дактилоскопическая идентификация.

Физическая защита объектов, как правило, предполагает усиление конструкций ограждений, элементов зданий, сооружений и отдельных помещений.

К таким средствам относятся защита оконных проемов металлическими решетками и ставнями, специальное остекление окон, использование бронированных дверей, запирающих устройств, сейфов для хранения средств вычислительной техники и носителей информации.

В соответствии с особенностями используемых помещений и территорий политика безопасности предприятия также может предусматривать расположение мест хранения и обработки информации (например, архивов или серверных комнат) в помещениях, наименее доступных для проникновения, наиболее удаленных от мест хранения взрывоопасных и легковоспламеняющихся веществ, наименее подверженных затоплению (для объектов расположенных в долинах рек и на побережье), наиболее защищенных от ударов молнии и т.п.

С физической защитой непосредственно связано **использование средств сигнализации и видеонаблюдения.** В зависимости от характера охраняемого объекта (территория, здание, проход, помещение, отдельный шкаф или сейф) в средствах сигнализации могут применяться датчики, работающие на различных физических принципах (фотоэлектрические датчики, датчики объема, аккустические датчики и т.п.), имеющие различные настройки и использующие различные каналы связи.

В отличие от средств сигнализации средства видеонаблюдения позволяют не только установить факт нарушения, но и в деталях отслеживать его, контролировать ситуацию, а также вести видеозапись, которую можно будет использовать для принятия дальнейших мер (поиск нарушителей, уголовное преследование и т.п.)

Отдельной задачей является **обеспечение информационной безопасности при процессе транспортировки** носителей информации и других объектов, требующее использования как специальных организационных приемов, так и специальных технических средств.

К организационным методам относится привлечение специально подготовленных курьеров, а также разделение носителей информации (объектов) на части и их раздельная транспортировка с целью минимизации возможностей утечки информации.

К техническим средствам, применяемым при транспортировке объектов, относятся защищенные контейнеры, специальные упаковочные материалы, а также тонкопленочные материалы и голографические метки, позволяющие идентифицировать подлинность объектов и контролировать несанкционированный доступ к ним.

Организация режима секретности в учреждениях и на предприятиях в РФ основывается на требованиях федерального законодательства, касающегося вопросов государственной тайны, и соответствующих подзаконных актов.

В соответствии с действующими нормами к государственной тайне может быть отнесена информация, касающаяся обороноспособности страны, ее экономики, международных отношений, государственной безопасности и охраны правопорядка (в том числе сведения о методах и средствах защиты секретной информации, а также о государственных программах и мероприятиях в области защиты государственной тайны); в законодательстве также специально уточняются области деятельности, информация о которых не может быть отнесена к государственной тайне.

Отнесение конкретной информации к государственной тайне производится решением специально назначаемых должностных лиц, а общий Перечень сведений, отнесенных к государственной тайне, утверждается Президентом РФ и подлежит обязательному опубликованию.

Для сведений, составляющих государственную тайну, устанавливаются три степени секретности: "особой важности", "совершенно секретно" и "секретно", а носители таких сведений (документы) должны иметь соответствующие реквизиты.

Основным элементом организации режима секретности является **допуск должностных лиц и граждан к сведениям, составляющим государственную тайну.** Он предполагает выполнение руководством предприятия и подразделений по защите государственной тайны (во взаимодействии с уполномоченными правоохранительными органами) следующих основных мероприятий.

- Ознакомление должностных лиц и граждан с нормами законодательства, предусматривающими ответственность за нарушение требований.

- Получение согласия на временные ограничения их прав в соответствии с законодательством.
- Получение согласия на проведение в отношении их проверочных мероприятий.
- Принятие решения о допуске к сведениям, составляющим государственную тайну.
- Заключение с лицами, получившими допуск, трудового договора (контракта), отражающего взаимные обязательства таких лиц и администрации предприятия (в т.ч. обязательства таких лиц перед государством по нераспространению доверенных им сведений, составляющих государственную тайну).

Важным элементом системы обеспечения режима секретности является **организация информационного обмена** между предприятиями при совместном выполнении работ.

В частности, **передача засекреченных сведений** от одного предприятия к другому должна производиться с разрешения уполномоченного государственного органа, договор на выполнение работ должен предусматривать обязательства сторон по обеспечению сохранности сведений, а заказчик работ должен контролировать выполнение нормативных требований контрагентами по таким договорам (наличие лицензий, оформление допуска сотрудников и т.п.) и принимать необходимые меры в случае выявления

Важным элементом обеспечения режима секретности является организация **передачи сведений, составляющих государственную тайну, другим государствам** (в том числе ознакомление с такими сведениями и предоставление возможности доступа к ним).

В каждом отдельном случае решение о передаче сведений выносится Правительством РФ на основании экспертного заключения Межведомственной комиссии по защите государственной тайны, которая, в свою очередь, руководствуется мотивированным ходатайством предприятия, заинтересованного в передаче секретных сведений, и решением органа государственной власти, курирующего круг вопросов, к которому относятся передаваемые сведения.

Для обеспечения защиты интересов РФ со стороной, принимающей секретные сведения, заключается договор, содержащий необходимые обязательства по защите получаемой информации, а также порядок разрешения конфликтных ситуаций и компенсации возможного ущерба .

Политика опубликования материалов в открытых источниках (таких как газеты, журналы, выставки, сеть Интернет, радио- и телепередачи, конференции, музейные экспозиции и т.п.) должна обеспечивать предотвращение случайных и организованных утечек конфиденциальной информации при взаимодействии предприятия со средствами массовой информации, общественными и государственными органами, научным, академическим и бизнес-сообществом.

Для того чтобы избежать ущерба интересам предприятия, такая политика должна содержать основные правила и процедуры подготовки информационных материалов к открытому опубликованию.

В частности, в политике безопасности следует предусматривать создание специального экспертного совета, ответственного за рассмотрение всех информационных материалов, которые предполагается опубликовать в открытых источниках (политика безопасности должна содержать конкретные ограничения на опубликование информационных материалов без их рассмотрения экспертным советом).

Основной задачей такого совета является подготовка заключений о возможности или невозможности опубликования определенных информационных материалов, а также подготовка конкретных предложений по изъятию определенных сведений из материалов, подготавливаемых к опубликованию.

При отсутствии единого мнения у членов экспертной комиссии решение о возможности опубликования может быть принято руководителем предприятия с учетом рекомендаций экспертов.

Для эффективного решения задач члены экспертного совета должны детально знать все существующие ограничения (в частности, установленные законодательством) и владеть ситуацией в той сфере, в которой функционирует предприятие.

При этом, как правило, сам автор подготавливаемых к опубликованию материалов не может входить в экспертный совет, а редактор или руководитель, отвечающий за подготовку материалов, не может быть председателем экспертного совета.

Характерным примером **политики использования сети Интернет** являются некоторые положения Указа Президента РФ от 12 мая 2004 года № 611 "О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена", регламентирующего вопросы подключения локальных сетей и персональных компьютеров к сети Интернет, а также размещение информации в сети Интернет для некоторых категорий пользователей. Данный документ:

- запрещает включение ИС, сетей связи и автономных персональных компьютеров, где обрабатывается информация, содержащая сведения, которые составляют государственную тайну, и служебная информация ограниченного распространения, а также для которых установлены особые правила доступа к информационным ресурсам, в состав средств международного информационного обмена, в том числе в сеть "Интернет";

- предписывает владельцам открытых и общедоступных государственных информационных ресурсов осуществлять их включение в состав объектов международного информационного обмена только при использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических для подтверждения достоверности информации].

Политика управления паролями (или, в более общем виде, политика идентификации и аутентификации) может определять периодичность замены паролей, действия, которые необходимо осуществить при компрометации паролей, основные требования к их качеству, процедурам их генерации, распределению основных обязанностей, связанных с генерацией паролей, их сменой и доведением до пользователей, а также основные меры ответственности за нарушение установленных правил и требований.

Политика на этом уровне также может устанавливать запрет хранения записанных паролей, запрет сообщать кому-либо свой пароль (в том числе руководителям и администраторам информационных систем) и другие аналогичные

Политика установки и обновления версий программного обеспечения может включать в себя некоторые ограничения на самостоятельное приобретение и установку программного обеспечения отдельными подразделениями и пользователями, а также определенные требования к квалификации специалистов, осуществляющих их установку, настройку и поддержку.

Политика приобретения информационных систем и их элементов (программных и аппаратных средств) может включать в себя требования к лицензированию и сертификации используемых программного обеспечения и оборудования, а также определенные требования к фирмам, осуществляющим их поставку и внедрение.

Политика доступа сторонних пользователей (организаций) в информационные системы предприятия может содержать перечень основных ситуаций, когда такой доступ возможен, а также основные критерии и процедуры, в соответствии с которыми осуществляется доступ.

Также политика может предусматривать распределение ответственности сотрудников самого предприятия за действия внешних пользователей, которые получают такой доступ.

Политика в отношении разработки ПО может содержать требования как к вопросам безопасности и надежности программных средств, самостоятельно разрабатываемых предприятием, так и в отношении передачи разработки программных средств (модулей информационных систем, отдельных программных библиотек и т.п.) сторонним специализированным организациям (т.н. "аутсорсинг"), а также в отношении приобретения и использования тиражируемых программных библиотек (модулей), распространяемых компаниями-производителями.

В частности, политика может содержать требования к тестированию самостоятельно разрабатываемого ПО, анализу его исходных кодов, описывать основные критерии надежности

Политики использования отдельных универсальных информационных технологий в масштабе всего предприятия могут включать в себя:

- политику использования электронной почты (e-mail);
- политику использования средств шифрования данных;
- политику защиты от компьютерных вирусов и других вредоносных программ;
- политику использования модемов и других аналогичных коммуникационных средств;
- политику использования Инфраструктуры публичных ключей;
- политику использования технологии Виртуальных частных сетей (Virtual Private Network – VPN).

Политика использования электронной почты может включать в себя как общие ограничения на ее использование определенными категориями сотрудников, так и требования к управлению доступом и сохранению конфиденциальности сообщений, а также к администрированию почтовой системы и хранению электронных сообщений.

Кроме того, политика может предусматривать:

- запрет на использование электронной почты в личных целях;
- специальные требования к отправке и получению присоединенных файлов, которые потенциально могут содержать вредоносные программы;
- запрет на использование электронной почты временными сотрудниками;
- требования шифрования передаваемых сообщений;
- наблюдение за всеми передаваемыми и получаемыми сообщениями;
- ограничения на передачу конфиденциальной информации при помощи электронной почты и другие положения.

Политика использования коммуникационных средств может определять границы использования технологий, позволяющих подключить компьютеры и информационные системы предприятия к информационным системам и коммуникационным каналам за его пределами.

В частности, такая политика может вводить определенные ограничения на использование модемов для телефонных линий, устройств, использующих современные беспроводные технологии, такие, как GSM (GPRS), Wi-Fi, передача данных

Политика использования мобильных аппаратных средств может относиться к различным устройствам, таким как мобильные ПК, КПК (PDA), переносные устройства хранения информации (дискеты, USB-flash, карты памяти, подключаемые жесткие диски и т.п.).

Она может отражать общее отношение предприятия к использованию сотрудниками таких устройств, определять требования и устанавливать конкретные области, в которых их использование допустимо.

Также могут устанавливаться дополнительные общие требования к стационарному оборудованию в целях ограничения подключения к ним мобильных компьютеров и средств переноса данных.

Политика информационной безопасности предприятия: нижний уровень

Данный уровень включает в себя документы, являющиеся инструкциями и методиками прямого действия, используемыми в повседневной деятельности сотрудников предприятия. Эти документы относятся к отдельным сервисам, процедурам и информационным системам.

Основной задачей разработки организационной документации на этом уровне является обеспечение как можно более детального и формализованного описания всех процедур и требований, относящихся к обеспечению безопасности отдельных элементов информационных систем, информационных потоков и массивов информации.

В частности, для обеспечения полноты формирования политики информационной безопасности предприятия необходимо сформировать как можно более полный комплект организационной документации, включающий в себя:

- бланки типовых заявок на предоставление доступа отдельных сотрудников к определенным информационным ресурсам и информационным системам, а также регламенты предоставления такого доступа;
- регламенты (процедуры) работы с определенными информационными и телекоммуникационными системами, программным обеспечением и базами данных;
- должностные обязанности отдельных категорий сотрудников в отношении обеспечения информационной безопасности, а также требования, предъявляемые к персоналу;
- типовые договоры с внешними контрагентами, связанные с передачей или получением информации, или основные требования, предъявляемые к таким договорам.

Процедурные документы, относящиеся к предоставлению доступа к ресурсам (таким как сеть Интернет, корпоративные информационные системы и базы данных, аппаратные средства, средства передачи информации и т.п.) могут включать как типовые бланки заявок на предоставление доступа, так и описание основных процедур (регламента) принятия решений о предоставлении такого доступа и предоставлении конкретных прав при работе с информационными ресурсами, а также перечни критериев, необходимых для предоставления тех или иных прав в информационных системах.

Процедуры работы с отдельными информационными системами и/или модулями информационных систем (базами данных, модулями корпоративной ERP-системы, системами электронного документооборота и т.п.) могут перечислять все основные требования, правила и ограничения, например, запрет использовать дискеты для копирования и переноса информации или ограничения, налагаемые на возможность удаленного доступа к тем или иным информационным сервисам.

Требования и правила, связанные с обеспечением информационной безопасности, могут быть как включены в общие инструкции по использованию информационных систем или регламенты осуществления бизнес-процессов, так и оформлены в виде специальных инструкций и памяток, содержащих исключительно требования и правила информационной безопасности.

Должностные обязанности персонала предприятия, связанные с обеспечением информационной безопасности, должны входить как составная часть в должностные инструкции для каждого сотрудника.

Кроме того, политика безопасности может предусматривать подписание (как при поступлении на работу или переводе на определенную должность, так и при увольнении с нее) отдельными категориями персонала дополнительных соглашений, обязательств и подписок о неразглашении определенной информации.

Также политика безопасности может вводить дополнительные требования к персоналу, работающему с определенными сведениями или информационными системами. Примерами таких ограничений могут быть отсутствие судимости, наличие определенных навыков или специальной квалификации, прохождение профессиональной сертификации или психологической проверки.

Политики безопасности, относящиеся к работе с внешними контрагентами, могут предусматривать типовые формы и отдельные инструкции по составлению коммерческих контрактов (для каждого типа контрактов, а также для отдельных групп контрагентов) и обмену информацией с поставщиками, покупателями, консультантами, посредниками, субподрядчиками, поставщиками финансовых и информационных услуг и другими участниками хозяйственной деятельности.

В частности, в политике для каждой из этих категорий может предусматриваться специфический порядок информационного обмена, взаимные требования по обеспечению конфиденциальности и возможные меры ответственности в случае нарушения согласованных требований какой-либо из сторон.

В тех случаях, когда определенная политика безопасности описывает сложную информационную систему и систему защиты информации, предназначенную для выполнения наиболее ответственных операций (таких как, например, электронные денежные переводы), она может быть разделена на две составляющие:

- внутренний регламент работы подразделений (групп, администраторов), отвечающих за выполнение наиболее важных административных функций (например, выдача и обслуживание электронных сертификатов Инфраструктуры публичных ключей);
- политику, непосредственно отражающую требования к пользователям и процессам, а также описания процедур работы и взаимодействия всех участников информационного обмена.

В этом случае внутренний регламент может содержать подробное описание тех правил и требований, которые должны выполнять ответственные подразделения (ИТ-служба, Департамент информационной безопасности или Служба безопасности предприятия) в процессе выполнения своих функций.

Такой регламент может быть необходим для демонстрации надежности наиболее важных и ответственных элементов инфраструктуры информационной безопасности. Это особенно важно в том случае, если предприятие осуществляет информационный обмен с внешними контрагентами (и, в частности, клиентами) и демонстрация надежности внутренних процедур сервисов информационной безопасности может обеспечить расширение бизнеса и повышение эффективности отдельных операций.

В некоторых случаях объем таких документов (политик, регламентов) может достигать нескольких десятков страниц (как правило, не более 100-150 страниц). Документы такого размера, как правило, составляются в тех случаях, когда может понадобиться их использование в судебных процессах для установления степени вины и ответственности различных участников процедур информационного обмена.

В том случае, если отдельные политики представляют собой сложные объемные документы, изобилующие юридическими и техническими терминами, они могут сопровождаться дополнительным документом, кратко раскрывающим основные требования и положения для большинства пользователей.

Такой документ должен иметь относительно небольшой объем (например, не более двух страниц) и содержать описание наиболее важных аспектов предмета политики: практически важные ограничения, ответственность и основные правила, знание которых необходимо для повседневной деятельности.

К числу документов на среднем и нижнем уровне детализации, помимо собственно политик безопасности, можно отнести также юридическое заключение, формально подтверждающее, что все меры информационной безопасности, предпринимаемые на предприятии, соответствуют требованиям действующего законодательства и/или стандартов.