

1 Внутриобъектовый режим; охрана помещений и территорий

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 пр.;
- 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 пр.;
- 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 опознавание 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 пр.) либо на основе считывания и анализа его физических особенностей (геометрии лица, отпечатков пальцев, рисунка радужной оболочки глаза, голоса и пр.). 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 пр.

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, акустические датчики и пр.), 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 пр.).

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.

2 Физическая защита объектов

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 пр.

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

Тема 2.6 – Управление информационной безопасностью предприятия
(Управление информационной безопасностью)

средствах сигнализации могут применяться датчики, работающие на различных физических принципах (фотоэлектрические датчики, датчики объема, акустические датчики и пр.), 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 пр.).

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.

3 Организация режима секретности

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:

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

- 2) Получение согласия на временные ограничения их прав в соответствии с законодательством.

3) Получение согласия на проведение в отношении их проверочных мероприятий.

4) Принятие решения о допуске к сведениям, составляющим государственную тайну.

5) 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).

Помимо отнесения сведений к государственной тайне и допуска должностных лиц и граждан к засекреченным сведениям, 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 пр.) и принимать необходимые меры в случае выявления нарушений.

Также 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 стороны, принимающей секретные сведения, заключается договор, содержащий необходимые обязательства по защите получаемой информации, а также порядок разрешения конфликтных ситуаций и компенсации возможного ущерба.

4 Характеристики политик безопасности

4.1 Политика опубликования материалов в открытых источниках

Политика опубликования материалов в открытых источниках (таких как газеты, журналы, выставки, сеть Интернет, радио- и телепередачи, конференции, музейные экспозиции и пр.) 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 информационных систем, 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.

4.2 Политика управления паролями

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 ограничения.

4.3 Политика установки и обновления версий программного обеспечения

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.

4.4 Политика приобретения информационных систем и их элементов

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.

4.5 Политика доступа сторонних пользователей (организаций)

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.

4.6 Политика в отношении разработки ПО

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 пр.) 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 и пр.

4.7 Политики использования отдельных универсальных информационных технологий

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;

Тема 2.6 – Управление информационной безопасностью предприятия
(Управление информационной безопасностью)

- 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.

4.8 Политика использования коммуникационных средств

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 в сетях стандарта CDMA и пр.

4.9 Политика использования мобильных аппаратных средств

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 пр.). 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.