Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студентка: Коржова Валерия Сергеевна

ФИТ 2 курс 4 группа

Минск 2022

**Практическое занятие №3**

**Тема «Разработка политики информационной безопасности бизнес-компании»**

Цель: Разработать проект политики информационной безопасности бизнес-компании.

**Введение**

Так что же такое информационная безопасность? Обычно под ней понимают защищенность информации и всей компании от преднамеренных или случайных действий, приводящих к нанесению ущерба ее владельцам или пользователям. Обеспечение информационной безопасности должно быть направлено прежде всего на предотвращение рисков, а не на ликвидацию их последствий. Именно принятие предупредительных мер по обеспечению конфиденциальности, целостности, а также доступности информации и является наиболее правильным подходом в создании системы информационной безопасности.

Любая утечка информации может привести к серьезным проблемам для компании — от значительных финансовых убытков до полной ликвидации. Конечно, проблема утечек появилась не сегодня, промышленный шпионаж и переманивание квалифицированных специалистов существовали еще и до эпохи компьютеризации. Но именно с появлением ПК и интернета возникли новые приемы незаконного получения информации. Если раньше для этого необходимо было украсть и вынести из фирмы целые кипы бумажных документов, то сейчас огромные объемы важных сведений можно запросто слить на флэшку, помещающуюся в портмоне, отправить по сети, прибегнув к использованию семейства руткитов, троянов, бэкдоров, кейлоггеров и ботнетов, либо просто уничтожить посредством вирусов, устроив диверсию.

Чаще всего «утекают» из компаний документы финансового характера, технологические и конструкторские разработки, логины и пароли для входа в сеть других организаций. Но серьезный вред может нанести и утечка персональных данных сотрудников. Особенно это актуально для западных стран, где судебные иски из-за таких утечек нередко приводят к огромным штрафам, после выплаты которых компании терпят серьезные убытки.

**\**

**Описание структуры завода**

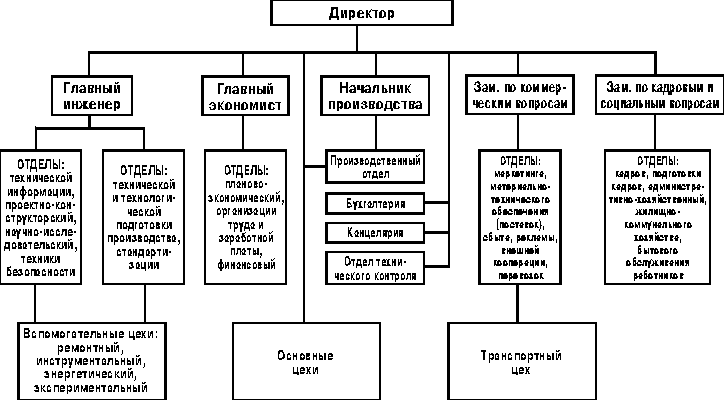


Рис.1 Завод

Организационная структура менеджмента машиностроительного предприятия зависит от многих факторов, и в первую очередь от масштаба и типа производства, сложности выпускаемой продукции, уровня механизации и автоматизации производства и управления, отраслевого уровня кооперации, численности работающих и др. Однако, общность принципов, методов и задач менеджмента позволяют разрабатывать типовые организационные структуры, свойственные среднему по размеру предприятию машиностроения.

Как правило, на таких предприятиях используется линейнофункциональная, трехступенчатая организационная структура менеджмента (предприятие - цех - участок) и соответственно линейный персонал - директор предприятия, начальник цеха, мастер.

На крупных предприятия может быть использована корпусная производственная структура (в корпусе размещаются несколько цехов), тогда количество уровней (ступеней) может быть увеличено до четырех и более.

На небольших предприятиях, как правило, организуется бесце- ховая производственная структура, и как следствие широко используется двухступенчатая организационная структура менеджмента предприятия.

Всей производственно-хозяйственной деятельностью на средних по размеру предприятиях машиностроения на высшем уровне иерархической структуры руководит директор (генеральный директор) и его заместители (рис. 9.7).

Директор организует всю работу предприятия и несет полную ответственность за его состояние, результаты деятельности и качество выпускаемой продукции. Ему непосредственно подчинены главный инженер, заместители: по производству, экономике (главный экономист), общим вопросам, качеству продукции и др.

Главный инженер является первым заместителем директора и осуществляет производственно-техническую политику предприятия, руководит процессами создания и освоения новой техники и новой технологии, повышения качества выпускаемой продукции, организации работ по рационализации и изобретательству и др. У главного инженера имеется, как правило, 2 заместителя.

Первый зам. главного инженера руководит работой функциональных подразделений, занимающихся технической подготовкой производства, в частности: отделом главного конструктора, отелом главного технолога, отделом технической документации, отделом научно-технической информации, инструментальным отделом, отделом рационализации и изобретательства, патентным бюро, экспериментальным цехом.

**Оценка рисков**

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения:

* антропогенные,
* техногенные,
* естественные (природные).

Возникновение *антропогенных* угроз обусловлено деятельностью человека. Возникновение *техногенных* угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. Возникновение *естественных (природных)* угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

Источники угроз по отношению к инфраструктуре рекламного агентства могут быть как внешними, так и внутренними.

*Внутренние:*

* несанкционированный доступ в помещение;
* возможность записи информации на переносные устройства (флэш карты, съемные жесткие диски и т.п.);
* пересылка фотоснимков с бумажных носителей и экранов мониторов с помощью мобильных телефонов, фотокамер и другими способами;
* компьютерные вирусы и «троянские» программы;
* незаконное получение и распространение за пределами предприятия лицензионных программ для предприятия;
* не контролируемая электронная почта;
* вынос техники предприятия, без соответствующего документа;
* внос посторонней техники на территорию предприятия.

*Внешние:*

* несанкционированный доступ из сети Интернет;
* снятие информации с кабельных систем (ЛВС и электропитания) при помощи технических средств;
* запись разговоров на расстоянии сквозь стены (окна, двери) и т.д.;
* установка прослушивающих устройств в помещениях.

*Непреднамеренные искусственные угрозы:*

* Неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (удаление, искажение файлов с важной информацией или программ);
* неумышленная порча носителей информации;
* ввод в систему ошибочных данных в силу некомпетентности;
* заражение компьютера вирусами (случайное);
* неосторожные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной;
* игнорирование организационных ограничений (установленных правил);
* некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом средств защиты;
* неумышленное повреждение каналов связи.

*Преднамеренные искусственные угрозы:*

* отключение или вывод из строя (путем взрыва, поджога и т.п.) подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
* несанкционированный доступ в помещения для совершения кражи или других действий в не рабочее время;
* нарушение конфиденциальности при электронной почтовой пересылке;
* нарушение апеллируемости при электронной почтовой пересылке.

*Естественные угрозы:*

* пожары;
* прорыв трубы, протечка в крыше.

**Разработка мер защиты**

Техническое обеспечение включает технологии, механизмы и средства, позволяющие реализовать заданный уровень информационной безопасности каждой конкретной сети, информационной системы, ресурса, автоматизированного рабочего места компонентов информационной инфраструктуры путем выполнения комплекса организационно-технических мероприятий.

Методами и способами защиты информации от несанкционированного доступа являются:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также, хранятся носители информации;

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

- резервирование технических средств, дублирование массивов и носителей информации;

- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

- использование защищенных каналов связи;

- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

На практике обеспечение информационной безопасности фирмы осуществляется с помощью следующих средств:

Моральные средства защиты

Под моральными средствами подразумевают нормы поведения и правила работы с информационными активами, сложившиеся по мере распространения и внедрения электронной техники в различных отраслях государства и общества в целом.

К морально-этическим средствам защиты информации в первую очередь стоит отнести честность и порядочность сотрудников. В каждой организации есть свой свод правил и предписаний, направленный на создание здорового морального климата в коллективе. Механизмом обеспечения безопасности служит внутренний документ компании, учитывающий особенности деловых процессов и информационной структуры, а также устройство IT-системы.

Правовые средства защиты

Они основываются на действующих стране законах, решениях и нормативных актах, устанавливающих правила обработки персональных данных, гарантирующих права и обязанности участникам при работе с информационными ресурсами в период их обработки и использования, а также возлагающих ответственность за нарушение этих постановлений, тем самым устраняя угрозу несогласованного использования конфиденциальной информации. В основном это организованные пояснительные беседы с персоналом предприятия, пользующимся корпоративными электронными устройствами.

Организационные средства

Это часть администрирования организации. Основной целью организационных мер является формирование внутренней политики в области сохранения в секрете конфиденциальных данных, включающей использование необходимых ресурсов и контроль за ними.

Внедрение политики конфиденциальности включает реализацию средств контроля и технических устройств, а также подбор персонала службы внутренней безопасности. Возможны изменения в устройстве IT-системы, поэтому в реализации политики конфиденциальности должны участвовать системные администраторы и программисты. Персонал должен знать, почему проблемы сохранения коммерческой тайны столь важны. Все работники предприятия должны пройти обучение правилам работы с конфиденциальной информацией.

Физические средства защиты

Это различные типы механических и электронно-механических устройств для создания физических препятствий при попытках нарушителей воздействовать на компоненты автоматизированной системы защиты информации. Это также технические устройства охранной сигнализации, связи и внешнего наблюдения. Средства физической безопасности направлены на защиту от стихийных бедствий, пандемий, военных действий и других внезапных происшествий.

Аппаратные средства защиты

Это электронные устройства, интегрированные в блоки автоматизированной системы или спроектированных как независимые устройства, контактирующие с этими блоками. Их задачей является внутренняя защита структурных компонентов ИТ-систем – процессоров, терминалов обслуживания, второстепенных устройств. Реализуется это с помощью метода управления доступом к ресурсам (идентификация, аутентификация, проверка полномочий субъектов системы, регистрация).

Программные методы защиты

Обеспечение сетевой безопасности осуществляется за счет специальных программ, которые защищают информационные ресурсы от несанкционированных действий. Благодаря универсальности, простоте пользования, способности к модифицированию программные способы защиты конфиденциальных данных являются наиболее популярными. Но это делает их уязвимыми элементами информационной системы предприятия. Сегодня создано большое количество антивирусных программ, брандмауэров, средств защиты от атак.

Путем использования перечисленных категорий программ, подходящим к используемым на предприятии информационным системам, создается комплексное обеспечение сетевой безопасности.

**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.

Опыт показывает, что для достижения удачных решений по защите информации кампаний необходимо сочетание правовых, организационных и технических мер. Это сочетание определяется конфиденциальностью защищаемой информации, характером опасности и наличием средств защиты. В общем случае технические меры безопасности составляют незначительную часть от общих мер защиты (правовых и организационных). Однако ни одну из них упускать нельзя. Каждая мера дополняет другую, и недостаток или отсутствие любого способа приведёт к нарушению защищённости.

Особое внимание при оценке эффективности системы защиты техническими средствами необходимо обратить на их надёжность и безотказность. При их эксплуатации имеют место поломки, сбои, отказы, вследствие чего они не обеспечивают выполнение задачи защиты. Отсюда задача обеспечения надлежащей надёжности технических средств обретает значительную важность, так как уровень, качество и безопасность защиты находятся в прямой зависимости от надёжности технических средств.