Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студентка: Сятковская Е. Д.

ИТ 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**

В век информационных технологий мы имеем выбор хранения информации, таким образом мы можем хранить её:

* На бумажных носителях;
* На различных цифровых носителях.

Каждый день мы используем устройства, из которых мы считываем довольно большие объёмы информации, либо заносим туда свою информацию, которая может быть сугубо личной, либо открытой для всех, так же это относится и к компании. Так что главной задачей для всех является защита своей информации, что является довольно сложной задачей в связи с развитием технологий и появлением глобальной сети. Модели угроз и нарушителей должны быть основным инструментом менеджмента нашей организации при развертывании, поддержании и совершенствовании системы обеспечения информационной безопасности организации.

Информационные ресурсы в современном обществе являются наиболее значимыми, но при этом, очень уязвимыми т.к. механизм их распространения становится все более гибким и количество возможностей их передачи растет. В связи с этим информационная безопасность — одно из важнейших условий функционирования любой структуры, будь то государственное учреждение или частное предприятие.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Беларуси. Поэтому решение вопроса об разработке эффективной политики информационной безопасности на современном предприятии обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации.

Пока не существует формальных методов нейтрализации угроз безопасности информации. По этой причине разработка мер по защите информации должна производиться на основе знаний и опыта соответствующих специалистов (каждый член бригады, выполняющей лабораторную работу, является специалистом - экспертом по защите конфиденциальной информации). Однако в интересах минимизации ошибок процесс разработки должен соответствовать следующим рекомендациям.

Разработку мер защиты информации целесообразно начинать с угроз, имеющих максимальное значение; далее - с меньшей угрозой, и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы. Такой подход гарантирует, что даже при малых ресурсах хватит ресурсов для предотвращения наиболее значимых угроз. Для каждой угрозы разрабатываются меры (способы и средства) по защите информации.

**Описание структуры рекламного агентства**

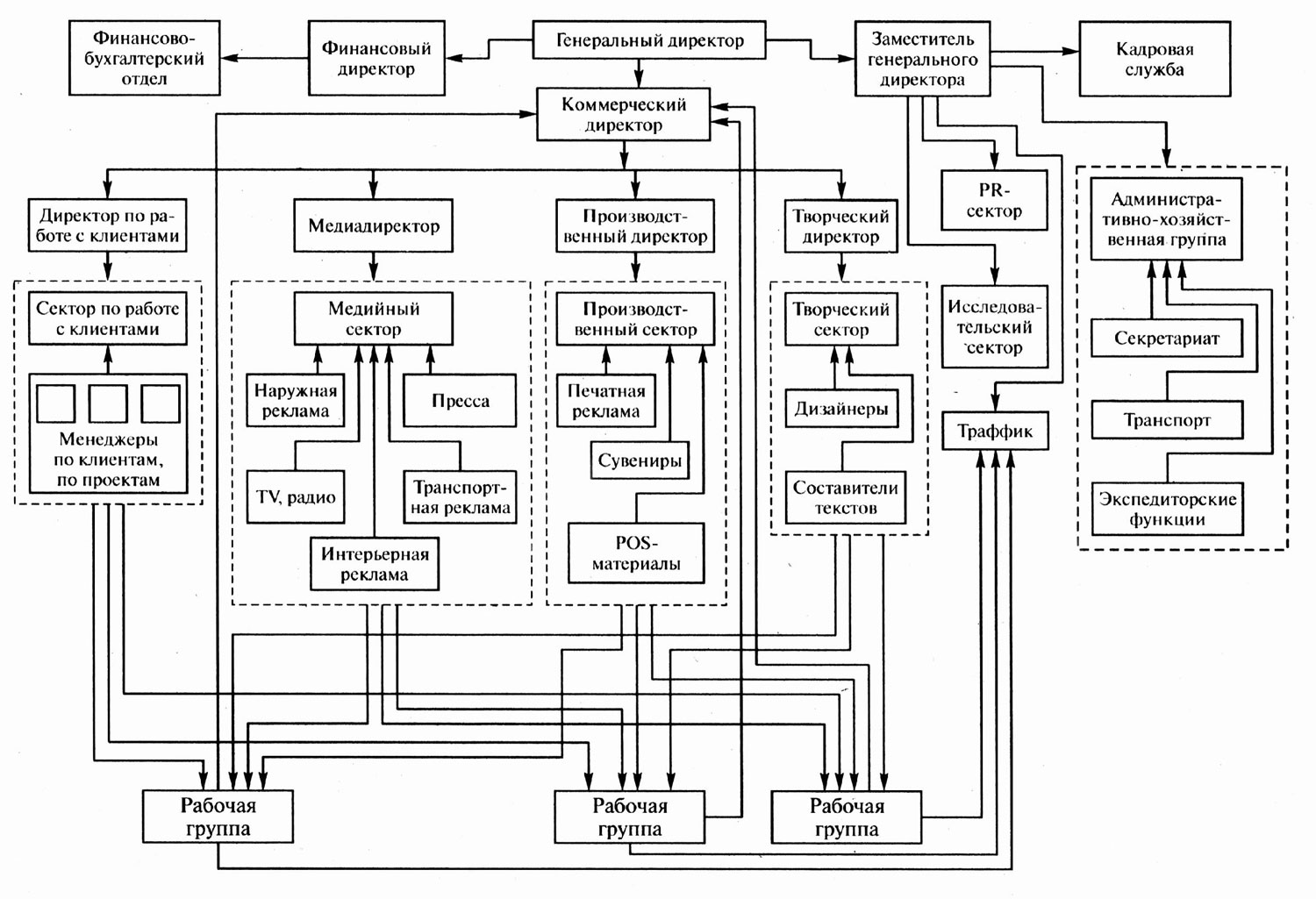


Рис.1 Структура рекламного агентства

Организационная структура кампании состоит из следующих основных отделов:

* Генеральный директор;
* Коммерческий директор;
* Директор по работе с клиентами;
* Творческий директор;
* Медиа директор;
* Производственный директор.

Таким образом, вся деятельность кампании, связанная с реализацией проектов, сосредоточена в этих отделах.

Наряду с основными отделами в кампаниях действует ряд обслуживающих отделов:

* Кадровая служба;
* Финансово-бухгалтерский отдел;
* Административно-хозяйственная группа.
* И т.д.

*Генеральный директор* — осуществляет общее руководство кампанией.

*Коммерческий директор* — сотрудник который, курирует работу нескольких отделов, чтобы компания развивалась по общей траектории и все подразделения работали сообща.

Эффективность управления деятельностью зависит оттого, насколько грамотно сформирована организационная структура управления и насколько она соответствует цели деятельности организации.

В настоящее время под организационной структурой понимается упорядоченная совокупность устойчиво взаимосвязанных элементов, обеспечивающих функционирование и развитие организации как единого целого. Структура управления определяется также как форма разделения и кооперации управленческой деятельности. Можно сказать, что структура управления есть не что иное, как оптимальное распределение работы, прав и ответственности, порядка и форм взаимодействия между членами коллектива организации.

Составляющими организационных структур являются:

* элементы организационных структур управления — службы или органы аппарата управления, а также отдельные работники этих служб (органов);
* организационные отношения — отношения (связи) между подразделениями организации, уровнями ее управления, персоналом, посредством которых реализуются функции управления;
* уровни управления — совокупность прав, обязанностей и ответственности, характерная для должностных лиц, занимающих определенную ступень в иерархической структуре организации.

**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:

* моральных;
* правовых;
* организационных;
* физических;
* аппаратных;
* программных;
* технических;
* криптографических.

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.