Учреждение образования “БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ”

Практическая работа №1 «Разработка политики информационной безопасности бизнес-компании»

Выполнил:

студент 3 курса, 4 группы

Мозолевский Александр Дмитриевич

Проверила:

Копыток Дарья Владимировна

Минск 2023ПроТТеоре

**Практическая работа №1**

Цель: разработать проект политики информационной безопасности бизнес-компании

**Введение**

С развитием информационных технологий стали появляться новые методы хранения информации. На данный момент самым популярным способом хранения информации является хранение на различных цифровых носителях.

Также все развиваются устройства, которые способны считывать довольно большие объёмы информации, либо записывать её. Сама информация может быть сугубо личной, либо открытой для всех, также это относится и к компаниям. Поэтому перед людьми встает вопрос о защите этой информации от злоумышленников, что является довольно трудной 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, действующий 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. 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 военкомата**

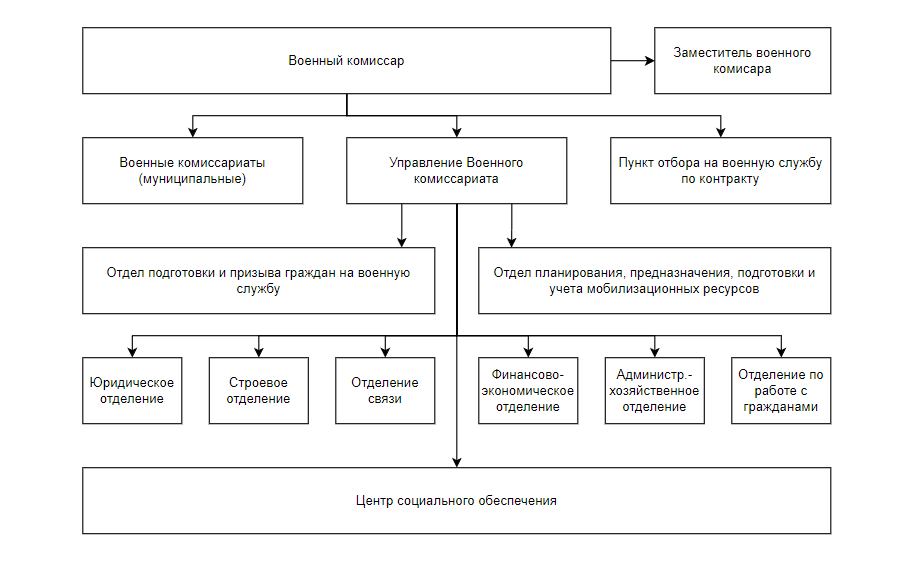


Рисунок 1.1. Структура ВК РБ

Организационная структура компании состоит из следующих основных лиц (отделов):

* Военный комиссар;
* Заместитель военного комиссара;
* Управление Военного комиссариата.

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

Наряду с основными лицами (отделами) в компаниях действует ряд обслуживающих отделов:

* Пункт отбора на военную службу по контракту;
* Отдел призыва граждан на военную службу;
* Юридическое отделение;
* Отделение по работе с гражданами;
* Центр социального обеспечения
* И т. д.

Военный комиссар – организует работу по взаимодействию военного комиссариата с органами исполнительной власти субъектов РБ, органами местного самоуправления и территориальными органами федеральных органов исполнительной власти.

Управление Военного комиссариата – отдел военного комиссариата, который отвечает за военно-мобилизационную и учётно-призывную работу в Вооружённых Силах РБ.

Эффективность управления деятельностью зависит от того, 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.

**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. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала, так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

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. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

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.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре Главпочтамта могут быть как внешними, так и внутренними.

Источниками внутренних угроз являются:

* Сотрудники организации;
* Программное обеспечение;
* Аппаратные средства.

К информационным угрозам относятся:

* Несанкционированный доступ к информационным ресурсам;
* Незаконное копирование данных в информационных системах;
* Противозаконный сбор и использование информации;
* Использование информационного оружия.

К программным угрозам относятся:

* Использование ошибок и «дыр» в программном обеспечении;
* Компьютерные вирусы и вредоносные программы.

К физическим угрозам относятся:

* Уничтожение или разрушение средств обработки информации и связи.

**Разработка мер защиты**

Всем сотрудникам компании, в которой установлена система контроля доступа, выдаются специальные электронные пропуска, представляющие собой пластиковые карты или брелоки, которые содержат персональные коды доступа. Считыватели, устанавливаемые у входа в контролируемое помещение, распознают код идентификаторов. Информация поступает в систему контроля доступа, которая на основании анализа данных о владельце идентификатора, принимает решение о допуске или запрете прохода сотрудника на охраняемую территорию. В случае разрешения доступа, система приводит в действие исполнительные устройства, такие как электромеханические замки, турникеты, автоматические шлагбаумы или приводы ворот. В противном случае двери блокируются, включается сигнализация и оповещается охрана.

Построение надежной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты.

Отдельный раздел законопроекта «О коммерческой тайне», посвященный организации защиты коммерческой информации, определяет необходимый комплекс мероприятий по ее защите:

* Установление особого режима конфиденциальности;
* Ограничение доступа к конфиденциальной информации;
* Использование организационных мер и технических средств защиты информации;
* Осуществление контроля за соблюдением установленного режима конфиденциальности.

Установление особого режима конфиденциальности направлено на создание условий для обеспечения физической защиты носителей конфиденциальной информации. Как правило, особый режим конфиденциальности подразумевает:

* Организацию охраны помещений, в которых содержатся носители конфиденциальной информации;
* Установление режима работы в помещениях, в которых содержатся носители конфиденциальной информации;
* Установление пропускного режима в помещениях, содержащих носителей конфиденциальной информации;
* Закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;
* Установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);
* Организацию ремонта технических средств обработки конфиденциальной информации;
* Организацию контроля за установленным порядком.

Эффективность защиты информации в автоматизированных системах достигается применением средств защиты информации (СЗИ). Под средством защиты информации понимается техническое, программное средство или материал, предназначенные или используемые для защиты информации. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

* Средства, обеспечивающие разграничение доступа к информации в автоматизированных системах;
* Средства, обеспечивающие защиту информации при передаче её по каналам связи;
* Средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;
* Средства, обеспечивающие защиту от воздействия программ-вирусов;
* Материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Радикальным способом защиты информации от утечки по физическим полям является электромагнитное экранирование технических устройств и помещений, однако это способ требует значительных капитальных затрат и практически не применяется.

Обеспечение требуемой защиты информационных ресурсов предприятий в этих условиях достигается применением дополнительных инструментальных средств. К их числу относятся средства анализа защищенности ОС и средства обнаружения опасных информационных воздействий в сетях.

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек и конфигурации установленным в организации. Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок, и проверка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей.

В информационной сфере с целью нейтрализации внутренних источников угроз национальной безопасности совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий. Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностям получения информационных услуг. Значимым этапом станет разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий. Особое внимание будет уделяться последовательному повышению качества, объема и конкурентоспособности национального контента, который призван занимать доминирующее положение внутри страны, и его продвижению во внешнее информационное пространство.

Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

Специалисты компании IBM выделяют четыре основных этапа построения системы безопасности:

* Идентификация информационных рисков и методов борьбы с ними;
* Описание мер защиты активов в соответствии с задачами и целями компании;
* Описание действий при происшествиях;
* Анализ остаточных рисков и принятие решения о дополнительном капиталовложении в методы обеспечения безопасности.

Ответ на вопрос «Что нужно защищать?» - основной аспект политики информационной безопасности, в соответствии со стратегией IBM. Политика должна создаваться с целью минимальных её изменений в будущем. Эффективная политика безопасности должна содержать:

* Цели и задачи обеспечения информационной безопасности;
* Взаимодействие со стандартами безопасности и законодательством;
* Расширение и ликвидация вирусных атак;
* Обеспечение непрерывности деятельности.

Далее идет процесс создания документации, которая содержит правила анализа рисков компании, описание рекомендуемых методов и средств защиты и так далее. Документация может подлежать изменениям в соответствии с актуальными уязвимостями и угрозами.

Однако, помимо правовой основы, система информационной безопасности и её функции по обеспечению состоянию защищенности объекта должны быть реализованы в соответствии с нижеизложенными принципами:

* Комплексность (разрабатываемая система защиты предусматривает комплексную реализацию методов, обеспечивает защиту информационных ресурсов на техническом и организационном уровнях и предотвращает возможные пути реализации угроз);
* Легитимность (создание системы информационной безопасности, а также реализация мероприятий по защите, не противоречащих законодательству и нормативам);
* Прогрессивность (подразумевает непрерывное развитие средств и методов защиты, в соответствии с развитием технологий и методов атак);
* Постоянность (обеспечивает непрерывную защиту объектов);
* Рациональность (использование экономически выгодных и эффективных средств защиты);
* Ответственность (каждый сотрудник ручается за обеспечение безопасности в рамках своих полномочий);
* Контроль (предполагает постоянных контроль над обеспечением защиты и своевременное выявление угроз);
* Этапность (проектирование системы безопасности делается поэтапно).

Проанализировав существующие политики и стандарты информационной безопасности можно утверждать, что для обеспечения надлежащего уровня информационной защиты требуется комплекс мер, включающий в себя функции программного обеспечения, политики безопасности, методы и организационные структуры. В соответствии с этим и с основной целью необходимо выполнить следующие задачи:

* Изучить исходную информационную и организационную структуру военкомата;
* По результатам анализа исходной информационной системы определить конкретные угрозы и уязвимости информационной безопасности;
* Определить уровень и класс исходной защищенности объекта;
* Выявить актуальные угрозы;
* Составить модель нарушителя;
* Сопоставить исходную систему с требованиями стандартов безопасности;
* Разработать политику безопасности.

Выполнение вышеизложенных целей и задач позволит создать эффективную систему информационной безопасности предприятия, отвечающую требованиям законодательства и стандартам информационной безопасности.

Нейтрализации ряда внутренних источников угроз национальной безопасности способствует информационное обеспечение государственной политики, которое заключается в доведении до граждан Республики Беларусь и внешней аудитории объективной информации о государственном курсе во всех сферах жизнедеятельности общества, официальной позиции по общественно значимым событиям внутри страны и за рубежом, о деятельности государственных органов. Важной задачей при этом является расширение каналов и повышение качества информирования зарубежной общественности. Составной частью информационного обеспечения государственной политики выступает информационное противоборство, представляющее собой комплексное использование информационных, технических и иных методов, способов и средств для воздействия на информационную сферу с целью достижения политических, экономических и иных задач либо защиты собственного информационного пространства.

Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий.

В интересах обеспечения национальной безопасности создается комплексная система стратегического планирования. Документы стратегического планирования, основой которых являются настоящая Концепция и программы социально-экономического развития Республики Беларусь, формируются, рассматриваются и утверждаются в порядке, предусмотренном законодательством.

Для защиты от внешних угроз национальной безопасности в научно-технологической сфере должно быть обеспечено проведение научных исследований и разработок в области приоритетных для Республики Беларусь технологий, их расширенное воспроизводство в структуре национальной экономики. Развитие индустрии проектирования компонентной базы производств высших технологических укладов обеспечит материально-техническую основу безопасности функционирования критически важных объектов, систем и инфраструктур.

Стратегическим фактором выступает развитие системы доступа к международным электронным базам данных научной и технической информации, создание системы международных научных лабораторий и центров, а также обеспечение наиболее благоприятных экономических и имиджевых условий для проведения исследований в Беларуси и привлечения инвестиций в ее научно-инновационную сферу, создания новых инновационных предприятий.

Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети. Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно, отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

В информационной сфере с целью нейтрализации внутренних источников угроз национальной безопасности совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий. Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностям получения информационных услуг. Значимым этапом станет разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий. Особое внимание будет уделяться последовательному повышению качества, объема и конкурентоспособности национального контента, который призван занимать доминирующее положение внутри страны, и его продвижению во внешнее информационное пространство.

Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

Нейтрализации ряда внутренних источников угроз национальной безопасности способствует информационное обеспечение государственной политики, которое заключается в доведении до граждан Республики Беларусь и внешней аудитории объективной информации о государственном курсе во всех сферах жизнедеятельности общества, официальной позиции по общественно значимым событиям внутри страны и за рубежом, о деятельности государственных органов. Важной задачей при этом является расширение каналов и повышение качества информирования зарубежной общественности. Составной частью информационного обеспечения государственной политики выступает информационное противоборство, представляющее собой комплексное использование информационных, технических и иных методов, способов и средств для воздействия на информационную сферу с целью достижения политических, экономических и иных задач либо защиты собственного информационного пространства.

Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий.

Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки на ВК, можем выделить следующие рекомендации, либо советы, следуя которым возможно снизить риски опасного воздействия и их последствий:

* Вооруженная охрана объектов и офисов компании;
* Четкая и строгая иерархия должностей и полномочий в компании;
* Обязательная экстренная связь каждого объекта с милицией и пожарной службой;
* Строгий подбор сотрудников;
* Защита главных серверов и почты ВК;
* Использование новейших средств защиты;
* Проведение инструктажей с сотрудниками;
* Наличие плана действий в случае чрезвычайных ситуаций.

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.

Целями защиты информации являются:

* Предотвращение утечки, хищения, утраты, искажения, подделки информации;
* Предотвращение несанкционированных действий по уничтожению, модификации, копированию информации;
* Предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

**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 компаний 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.