Практическая работа №9

ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Цель работы. Изучить структуру документа политики безопасности. Научиться составлять политику безопасности для информационного объекта.

Краткие сведения из теории

Высокая стоимость конфиденциальных сведений о деятельности конкурирующих структур показывает, что проблема ЗИ от перехвата ее техническими средствами и агентами конкурентов весьма актуальна как для государственного, так и негосударственного сектора. Особенно остро в настоящее время встает вопрос о необходимости защиты конфиденциальной информации негосударственного сектора. Это обусловлено тем, что государственный сектор давно серьезно занимался ЗИ и имеет в настоящее время солидный научно-технический потенциал, силы и технические средства для решения этих задач; негосударственный же сектор в вопросах ЗИ в стране делает первые шаги в отличие от государственного и частных фирм зарубежных стран, где этому вопросу уделяется большое внимание. Отсутствие подготовленных специалистов, научных проработок, опыта, знаний, необходимых документов и технических возможностей фирм у этого сектора в условиях конкуренции ставит их в затруднительное, неравное с предприятиями госсектора, положение.

Задача создания простых методических материалов, позволяющих руководителям грамотно организовать ЗИ на своих предприятиях, весьма актуальна.

Политика безопасности – совокупность норм, правил, рекомендаций, регламентирующих работу средств защиты ИО от фиксированного множества угроз безопасности.

Для определения области политики безопасности необходимо провести анализ угроз и рисков, классифицировать имеющиеся активы и размеры ущербов в случае их повреждения. На основе данного анализа составляют политику безопасности с целью уменьшить возможное проникновение угроз в систему.

Политика безопасности устанавливает правила, которые определяют конфигурацию систем, действия служащих организации в обычных условиях и в случае непредвиденных обстоятельств. Она заставляет людей делать вещи, которые они не хотят делать. Однако она имеет огромное значение для организации и является наиболее важной работой отдела информационной безопасности.

Определение способов развертывания системы безопасности, надлежа-

щих механизмов для защиты информации и систем, правильная настройка компьютерных систем и сетей в соответствии с требованиями физической безопасности – это все функции политики безопасности.

Политика устанавливает порядок осуществления служащими своих обязанностей, связанных с вопросами безопасности, определяет поведение пользователей при использовании компьютерных систем, размещенных в организации. И, самое главное, она устанавливает порядок реагирования в случае каких-либо непредвиденных обстоятельств. При нарушении безопасности или сбое в работе системы, политики и процедуры устанавливают порядок действий и выполнения задач, направленные на устранение последствий этого инцидента.

Исходя из положений международного стандарта ISO 17799, можно предложить следующую структуру типовой политики безопасности организации:

1 Общие положения.

1.1 Назначение документа.

1.2 Цели и задачи политики безопасности.

1.3 Нормативно-правовая база.

1.4 Основные определения.

2 Идентификация информационной системы.

2.1 Описание структурных подразделений

2.2 Идентификация активов.

2.3 Классификация информации по уровням секретности.

2.4 Идентификация уязвимостей ИС.

2.5 Идентификация угроз ИС.

2.6 Оценка рисков.

3.Меры информационной безопасности.

3.1 Средства физической безопасности и контроля территории.

3.2 Средства программно-технической защиты информации.

3.3 Средства обеспечения целостности информации.

3.4 Правила разграничения доступа сотрудников к информационным ресурсам.

3.5 Обеспечение безопасности при подключении к сети общего пользования.

4.Управление информационной безопасностью.

4.1 Аудит.

4.2 Осведомленность и обучение специалистов.

4.3 Сообщение об инцидентах информационной безопасности, реагирование и отчетность.

4.4 Должностные обязанности и ответственность.

В подразделе **«Назначение документа»** приводиться описание организации (структурного подразделения организации) и обосновывается необходимость защиты информации и составления политики безопасности.

Каждая политика и процедура имеют четко определенную цель, описывающую причины, почему создана та или иная политика или процедура, и какую выгоду от этого надеется получить организация.

Целью разработки официальной политики предприятия в области информационной безопасности является определение правильного (с точки зрения организации) способа использования вычислительных и коммуникационных ресурсов, а также разработка процедур, предотвращающих или реагирующих на нарушения режима безопасности. Чтобы достичь данной цели, следует учесть специфику конкретной организации.

Во-первых, необходимо принять во внимание цели и основные направления деятельности организации. Например, на военной базе и в университете существенно разные требования к конфиденциальности.

Во-вторых, разрабатываемая политика должна согласовываться с существующими законами и правилами, относящимися к организации. Значит, эти законы и правила необходимо выявить и принять во внимание при разработке политики.

В-третьих, если локальная сеть организации не является изолированной, вопросы безопасности следует рассматривать в более широком контексте. Политика должна освещать проблемы, возникающие на локальном компьютере из-за действий удаленной стороны, а также удаленные проблемы, причиной которых является локальный хост или пользователь.

К общим целям защиты информации относятся предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

Подраздел **«Нормативно-правовая база»** включает в себя перечень нормативных и правовых актов, используемых для написания политики безопасности и разъяснение соответствия положений политики местному и международному законодательству.

В случае если в политике безопасности встречаются нововведенные термины в подразделе **«Основные определения»** приводиться терминология.

В разделе **«Идентификация информационной системы»** классифицируются материальные и информационные ресурсы по их виду и уровню защиты. Также приводится перечень подразделений и должностей, работающих с материальными и информационными ресурсами, подлежащих защите, и отвечающих за работы в области информационной безопасности. В данном разделе представлены результаты идентификации уязвимостей, угроз и оценки рисков.

В разделе **«Меры информационной безопасности»** прописываются основные правила использования информационных и материальных активов с целью сохранения их целостности и недопущения несанкционированного

допуска.

В подразделе **«Средства физической безопасности и контроля территории»** могут приводиться регламентация допуска сотрудников в помещения, регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов. Например, системы хранения и передачи данных должны находиться в специальных помещениях, оборудованных надежными автоматическими замками, средствами сигнализации и постоянно быть под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов. В политике безопасности рекомендуется прописывать требования к средствам идентификации и аутентификации: какие системы должны использоваться для идентификации пользователей, какие пароли должны выбирать пользователи и др.

В подразделе **«Средства программно-технической защиты информации»** должен определяться список программных продуктов для обеспечения информационной безопасности, требования к ним и места для их обязательной установки (файловые серверы, рабочие станции и серверы электронной почты).

В политике безопасности устанавливаются стандартные требования к **управлению доступом** к электронным файлам, в которых предусматриваются формы управления доступом пользователей по умолчанию, доступные для каждого файла в системе. В разделе **«Правила разграничения доступа сотрудников к информационным ресурсам»** определяются разрешения на чтение, запись и исполнение, которые даются владельцам файлов и прочим пользователям системы.

Политика безопасности также описывает правила установки сетевых соединений и используемые механизмы защиты. Для соединений устанавливают технические правила аутентификации и аутентификации для каждого типа соединения (строгий контроль над разрешенными точками доступа). В качестве устройств защиты выделенных линий используют межсетевые экраны.

Политика безопасности должна определять механизмы, используемые при осуществлении удаленного доступа сотрудниками к внутренним системам. При этом политика безопасности должна определять процедуру прохождения авторизации для такого доступа. И самое главное при осуществлении удаленного доступа, чтобы все соединения были защищены шифрованием. Необходимо четко определять условия, при которых разрешается использование беспроводных соединений (если таковые имеются), и то, каким образом будет осуществляться авторизация в такой сети (дополнительные требования, предъявляемые к аутентификации или шифрованию).

В политике безопасности необходимо описывать правила по работе с системой электронной почты. Так, содержание электронных сообщений при

обмене документами с партнерами посредством электронной почты должно соответствовать корпоративным стандартам.

Аудит (auditing) – фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам.

Подсистема аудита современных ОС позволяет дифференцированно задавать перечень интересующих администратора событий с помощью удобного графического интерфейса.

Средства учета и наблюдения обеспечивают возможность обнаружить и зафиксировать важные события, связанные с безопасностью, или любые попытки создать, получить доступ или удалить системные ресурсы.

Подраздел **«Осведомленность и обучение специалистов»,** характеризующий меры безопасности, применяемые к персоналу, включает описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п. Пользователи информационной системы, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации.

Ключевым элементом политики является доведение до каждого его обязанностей по поддержанию режима безопасности. Политика не может предусмотреть всего, однако она обязана гарантировать, что для каждого вида проблем существует ответственный внутри каждого подразделения, который должен своевременно и правильно среагировать на любой инцидент. Для этого в подразделе **«Сообщение об инцидентах информационной безопасности, реагирование и отчетность»** описывается порядок действия сотрудников при нарушении информационной безопасности.

В разделе **«Должностные обязанности и ответственность»** определяются лица, ответственные за соблюдение политики безопасности и доведения до сведения сотрудников их обязанностей в области информационной безопасности. Дополнения к должностным обязанностям руководителей - ответственность за обеспечение информационной безопасности внутри подразделения, включая ответственность за предоставление отчетов об инцидентах.

В информационной безопасности можно выделить несколько уровней ответственности. На первом уровне каждый пользователь компьютерного ресурса обязан заботиться об информационной защите. Пользователь, допустивший компрометацию, увеличивает вероятность компрометации других ресурсов.

Системные администраторы или руководители подразделений образуют другой уровень ответственности. Они должны обеспечивать защиту компьютерных систем. Сетевых администраторов можно отнести к еще более вы-

сокому уровню.

В данном разделе также прописываются ответственности за нарушения установленного порядка пользования ресурсами информационной системы. Любое грубое нарушение порядка и правил пользования информационными ресурсами должно расследоваться. К виновным должны применяться адекватные меры воздействия.

Порядок выполнения работы

1 На основе данных, полученных в предыдущих практических работах, составить политику безопасности информационного объекта в соответствии с рекомендациями, изложенными в кратких сведениях из теории.

Содержание отчета

1 Цель работы.

2 Текст политики безопасности.

3 Вывод по работе.

Контрольные вопросы

1 Какие мероприятия необходимо проводить для внедрения политики безопасности?

2 Какие основные разделы должна включать политика безопасности?

3 Чем отличается идентификация пользователя от аутентификации?

4 Для чего необходим аудит?

5 Классификация информации.