Лабораторная работа 7

Политика безопасности

В этой работе Вы должны познакомиться с понятием «Политика безопасности», типовыми примерами политик и разработать собственный вариант политики безопасности для своего варианта предприятия.

Вариант предприятия можно взять из других дисциплин, где использовался проектный подход для выполнения практических заданий. При выборе предприятия надо руководствоваться, в первую очередь, хорошим знанием предметной области, а также архитектуры предприятия.

> ***Политика безопасности*** *— это совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.*

Такая трактовка, конечно, гораздо шире, чем набор правил разграничения доступа (именно это означал термин «security policy» в «Оранжевой книге» и в построенных на её основе нормативных документах других стран).

Политика безопасности строится на основе анализа рисков, которые признаются реальными для ИС организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т. п.

С практической точки зрения политику безопасности целесообразно рассматривать на трёх уровнях детализации.

К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации.

Примерный список подобных решений может включать в себя следующие элементы:

- Решение сформировать или пересмотреть комплексную программу обеспечения ИБ, назначение ответственных за продвижение программы.
- Формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей.
- Обеспечение базы для соблюдения законов и правил.
- Формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и её доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна чётко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров по VPN или технологию BYOD). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению её в жизнь. В этом смысле политика безопасности является основой подотчётности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины.

1. Организация должна *соблюдать существующие законы.*

2. Следует *контролировать действия лиц, ответственных за выработку программы безопасности.*
3. *Необходимо обеспечить определённую степень исполнительности персонала*, а для этого нужно выработать систему поощрений и наказаний.

На верхний уровень следует выносить минимум вопросов.

Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Политика информационной безопасности должна быть утверждена, издана и надлежащим образом доведена до сведения всех сотрудников организации. Она должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью.

Согласно ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью», **политика ИБ** должна включать, как минимум, следующие разделы:

- Определение информационной безопасности, её общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации.
- Изложение целей и принципов информационной безопасности, сформулированных руководством.
- Краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований.

  Например, наиболее существенные политики:

  1. Соответствие законодательным требованиям и договорным обязательствам;
  2. требования в отношении обучения вопросам безопасности;
  3. предотвращение появления и обнаружение вирусов и другого вредоносного программного обеспечения;
  4. управление непрерывностью бизнеса;
  5. ответственность за нарушения политики безопасности.
- Определение общих и конкретных обязанностей сотрудников в рамках управления ИБ, включая информирование об инцидентах нарушения ИБ.
- Ссылки на документы, дополняющие политику ИБ, например, более детальные политики и процедуры безопасности для конкретных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Средний уровень политики безопасности содержит вопросы, касающиеся отдельных аспектов ИБ, но важные для различных эксплуатируемых организацией систем. Примеры таких вопросов — отношение к передовым (но, возможно, недостаточно проверенным) технологиям, доступ в Интернет (как совместить свободу доступа к информации с защитой от внешних угроз?), использование домашних компьютеров и мобильных устройств, применение пользователями неофициального программного обеспечения и т. д.

Политика безопасности среднего уровня должна для каждого аспекта освещать следующие темы:

Описание аспекта информационной безопасности. Например, если рассмотреть применение пользователями неофициального программного обеспечения, последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

Область применения — следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на производственные машины?

Позиция организации по данному аспекту информационной безопасности. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приёмки подобного ПО и т. п. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще стиль документов, определяющих политику безопасности (как и их перечень), в разных организациях может сильно отличаться.

Роли и обязанности — необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность — политика должна содержать общее описание запрещённых действий и наказаний за них.

Точки контакта — должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно «точкой контакта» служит определённое должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она включает в себя два аспекта — *цели* и *правила их достижения*. Поэтому её порой трудно отделить от вопросов реализации.

Политика ИБ на этом уровне должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время, эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне.

Например, надо ответить на следующие вопросы:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?
- как организован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений *целостности*, *доступности* и *конфиденциальности*.

Её цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать.

Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жёсткие правила могут мешать работе пользователей, вероятно, их придётся часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

Задание 1. Знакомство с примерами политики безопасности

Познакомьтесь с примерами политики безопасности из открытых источников. Постарайтесь найти пример для наиболее близкой (по предметной области и архитектуре) компании.

Задание 2. Разработка политики безопасности

Создайте свой документ «Политика безопасности», взяв за основу наиболее близкий пример. Используйте известную Вам информацию о предметной области и о предприятии.

Полученный документ (в формате PDF) загрузите на Moodle.