Лекция 3. Административные меры защиты информации

Вопросы:

1. ***Цели, задачи и содержание административного уровня***
2. ***Политика безопасности***
3. ***Программа безопасности***
4. ***Анализ и управление рисками***

1. Цели, задачи и содержание административного уровня

Главная цель мер административного уровня – сформировать программу работ в области ИБ и обеспечить ее выполнение в конкретных условиях функционирования ИС, выделяя необходимые ресурсы и контролируя состояние дел.

Основная задача мер административного уровня – разработка и реализация практических мероприятий по созданию системы обеспечения ИБ, учитывающей особенности защищаемых ИС.

Содержанием административного уровня являются следующие мероприятия:

- разработка политики безопасности;
- составление программы безопасности;
- проведение анализа угроз и расчета информационных рисков;
- выбор механизмов и средств обеспечения ИБ.

Под *политикой безопасности* понимается совокупность документированных решений, принимаемых руководством организации и направленных на ЗИ и ассоциированных с ней ресурсов. Политика безопасности – это не отдельные правила или их наборы (такого рода решения выносятся на процедурный уровень), а стратегия организации в области ИБ.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации.

Когда риски проанализированы, и стратегия защиты определена, составляется программа обеспечения ИБ. Под нее выделяются ресурсы, назначаются ответственные лица, определяется порядок контроля выполнения программы.

2. Политика безопасности

Политика безопасности – это комплекс предупредительных мер по обеспечению ИБ организации, включающая руководящие принципы, правила и процедуры в области безопасности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений.

Основные направления разработки политики безопасности:

- определение объема и требуемого уровня защиты данных;
- определение ролей субъектов информационных отношений.

Результатом разработки политики безопасности является комплексный документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения ИБ.

1) основные положения ИБ организации (определяют важность ОБИ, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы);

2) область применения политики безопасности (перечисляются компоненты ИС обработки, хранения и передачи информации, подлежащие защите);

3) цели, задачи и критерии оценки ИБ (определяются функциональным назначением организации – для режимных организаций важно соблюдение конфиденциальности; для сервисных информационных служб реального времени важным является обеспечение доступности подсистем; для информационных хранилищ актуальным является обеспечение целостности данных и т.д.);

4) распределение прав и обязанностей субъектов информационных отношений организации (целесообразно провести по следующим ролям – владелец информации; руководитель подразделения; специалист по ИБ; администраторы сети и конкретных сервисов; пользователи; поставщики аппаратного и программного обеспечений; аудиторы; некоторые роли могут отсутствовать, некоторые – совмещаться в одном и

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

- верхний уровень – вопросы, относящийся к организации в целом;
- средний уровень – вопросы, касающиеся отдельных аспектов ИБ;
- нижний уровень – вопросы, относящиеся к конкретным сервисам.

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

- решение сформировать или изменить комплексную программу обеспечения ИБ, назначение ответственных за продвижение программы;
- формулирование целей организации в области ИБ, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулирование административных решений по вопросам, затрагивающим организацию в целом.

К среднему уровню относятся вопросы, касающиеся отдельных аспектов ИБ, но важные для различных эксплуатируемых организацией систем (отношения к передовым технологиям, доступа в Internet, использования домашних компьютеров, применения пользователями неофициального ПО и т.д.)

Политика среднего уровня для каждого аспекта освещает следующие темы:

1) Описание аспекта (основные понятия и определения);
2) Область применения (т.е. где, когда, как, по отношению к кому и чему применяется данная политика безопасности);
3) Позиция организации по данному аспекту (может быть сформулирована в конкретном или в более общем виде, как набор целей, которые преследует организация в данном аспекте);
4) Роли и обязанности (информация о должностных лицах, ответственных за реализацию политики безопасности);
5) Законопослушность (описание запрещенных действий и наказаний);
6) Точки контакта (должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией).

Политика безопасности нижнего уровня относится к конкретным информационным сервисам, включает в себя два аспекта – цели и правила их достижения. В отличие от двух верхних уровней, рассматриваемая политика должна быть определена более подробно. Есть много позиций, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации, но в то же время настолько важных для обеспечения режима безопасности, что решения по отношению к ним должны приниматься на управленческом, а не на техническом уровне.

Несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

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

3. Программа безопасности

Программу верхнего уровня возглавляет лицо, отвечающее за ИБ организации. Главными целями этой программы являются:

1) управление рисками (оценка рисков, выбор средств защиты);
2) координация деятельности в области ИБ, пополнение и распределение ресурсов;
3) стратегическое планирование;
4) контроль деятельности в области ИБ.

Контроль деятельности в области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать защитные меры с учетом изменения

Цель программы нижнего уровня – обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне:

- решается, какие следует использовать механизмы защиты;
- закупаются и устанавливаются технические средства;
- выполняется повседневное администрирование;
- отслеживается состояние слабых мест и т.п.

Обычно за программу нижнего уровня отвечают администраторы сервисов.

Программа безопасности нижнего уровня может быть синхронизирована с жизненным циклом защищаемого сервиса, что позволит добиться большего эффекта с меньшими затратами. Добавить новую возможность к уже готовой системе на порядок сложнее, чем изначально спроектировать и реализовать ее.

Основные этапы жизненного цикла информационного сервиса

1. Инициация. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.
2. Закупка. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.
3. Установка. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.
4. Эксплуатация. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.
5. Выведение из эксплуатации. Происходит переход на новый сервис.

4. Анализ и управление рисками

Основные понятия и этапы управления рисками

Риск – это возможность реализации угрозы вследствие наличия соответствующей уязвимости, приводящей к негативным последствиям (ущербу).

Ресурсы – объекты, представляющие ценность для обладающей ими организации. Могут быть материальными (tangible), например оборудование, локальная сеть и нематериальными (intangible), например счет в банке.

Угроза – возможная опасность случайного или преднамеренного действия, события, процесса, наносящего ущерб ресурсам, в отношении объекта защиты.

Уязвимость – любая характеристика ИС, использование которой источником угроз может привести к реализации угрозы.

Под *управлением рисками* понимается процесс идентификации, управления и уменьшения рисков безопасности, воздействующих на ИС. *Стоимость затрат на СЗИ* должна быть существенно меньше величины риска.

Этапы менеджмента риска (Risk Management):

оценка риска (Risk Assessment);

обработка риска (Risk Treatment);.

принятие риска (Risk Acceptance);

коммуникация риска (Risk Communication).

Оценка риска включает:

анализ риска (Risk Analysis), в том числе:

идентификацию рисков (Risk Identification);

расчет рисков (Risk Estimation);

оценивание риска (Risk Evaluation).

Обработка риска (Risk Treatment) – процесс выбора и осуществления мер по модификации риска. Осуществление мер включает:

оптимизацию (снижение) риска (Risk Optimization, Risk Reduction) – за счет использования дополнительных защитных средств;

предотвращение риска (Risk Avoidance) – за счет устранения причины;

перенос риска (Risk Transfer) – путем заключения страхового соглашения;

сохранение риска (Risk Retention).

Принятие риска (Risk Acceptance) – согласие с имеющимся риском и выработка плана действия в соответствующих условиях.

Коммуникация риска (Risk Communication) – обмен информацией о риске или совместное использование этой информации между лицом, принимающим решение, и другими причастными сторонами.

Выделяют два основных уровня анализа рисков:

базовый уровень: рассчитан на наиболее распространенные риски и соответствующие контрмеры (без оценки вероятностей угроз);

полный уровень: включает изучение бизнес-процессов компании, принятие во внимание реальных и потенциальных угроз и уязвимостей, предполагает использование качественных и количественных методик анализа рисков.

Анализ рисков может проводиться двумя способами:

качественным анализом – оценкой риска в условных единицах;

количественным анализом – оценкой риска в денежных единицах.

Этапы управления рисками:

1. Выбор анализируемых объектов и уровня детализации их рассмотрения.
2. Выбор методологии оценки рисков.
3. Идентификация активов.
4. Анализ угроз и их последствий, выявление уязвимых мест в защите.
5. Оценка рисков.
6. Выбор защитных мер.
7. Реализация и проверка выбранных мер.
8. Оценка остаточного риска.

Управление рисками – процесс циклический. По существу, последний этап – это оператор конца цикла, предписывающий вернуться к началу.

Управление рисками необходимо интегрировать в жизненный цикл ИС, тогда эффект оказывается наибольшим, а затраты – минимальными.

Что может дать управление рисками на каждом из этапов:

1) на этапе *инициации* известные риски следует учесть при выработке требований к системе вообще и средствам безопасности в частности;

2) на этапе *закупки* знание рисков поможет выбрать соответствующие архитектурные решения, играющие ключевую роль в обеспечении безопасности;

3) на этапе *установки* выявленные риски учитывают при конфигурировании, тестировании и проверке сформулированных требований, а полный цикл управления рисками должен предшествовать вводу системы в эксплуатацию;

4) на этапе *эксплуатации* управление рисками должно сопровождать все существенные изменения в системе;

5) при *выведении* системы из эксплуатации управление рисками помогает убедиться в том, что миграция данных происходит безопасным образом.

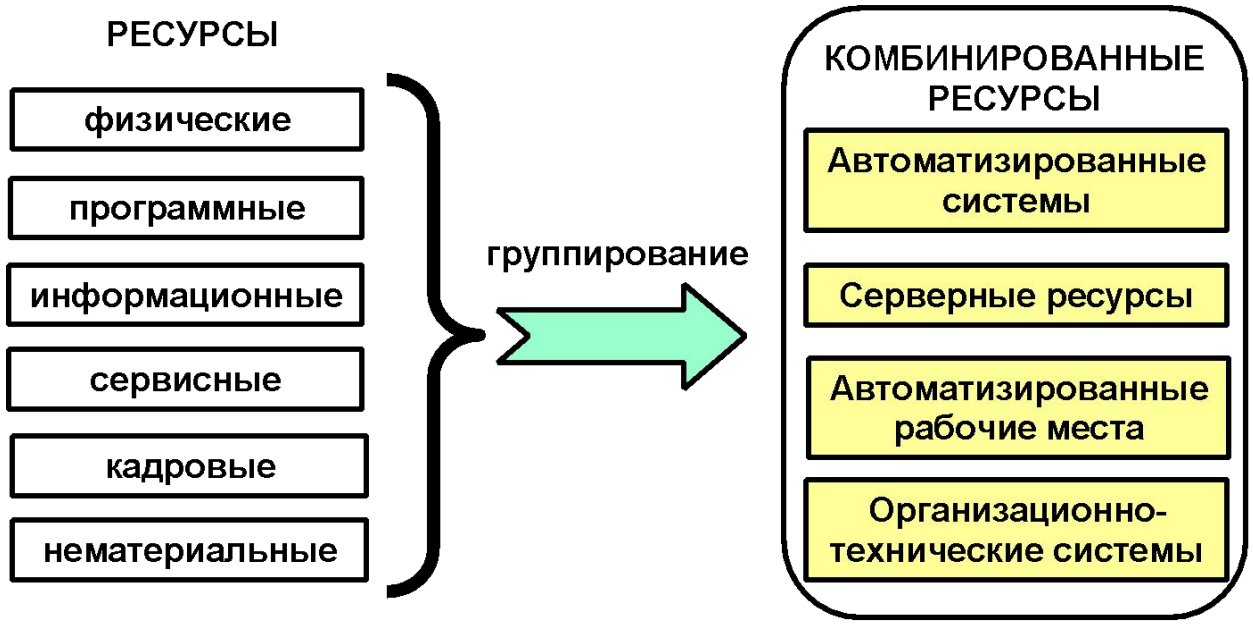
3 этап. При ***идентификации активов***, то есть тех ресурсов и ценностей, которые организация пытается защитить, следует учитывать не только компоненты ИС, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как репутация организации. Отправной точкой здесь является представление о миссии организации, то есть об основных направлениях деятельности, которые необходимо сохранить в любом случае.

4 этап. Рассматриваемые виды угроз следует выбирать, исходя из соображений здравого смысла (исключив, например, землетрясения, однако, не забывая о возможности захвата организации террористами), но в пределах выбранных видов провести максимально подробный анализ.

5 этап. После накопления исходных данных можно переходить собственно к оценке рисков. Допустимо применить такой простой метод, как умножение вероятности осуществления угрозы на предполагаемый ущерб. Если для вероятности и ущерба использовать трехбалльную шкалу, то возможных произведений будет шесть: 1, 2, 3, 4, 6 и 9. Первые два результата можно отнести к низкому риску, третий и четвертый – к среднему, два последних – к высокому, после чего появляется возможность снова привести их к трехбалльной шкале.

Идентификация и оценка активов, уязвимостей и угроз

Информационной основой крупной организации является сеть, поэтому в число аппаратных активов следует включить серверы, рабочие станции, периферийные устройства, внешние интерфейсы, кабельное хозяйство, активное сетевое оборудование.



Первый шаг в анализе угроз – их идентификация. Целесообразно выявлять не только сами угрозы, но и источники их возникновения – это поможет в выборе дополнительных средств защиты. После идентификации угрозы необходимо оценить вероятность ее осуществления. Допустимо использовать при этом трехбалльную шкалу (низкая (1), средняя (2) и высокая (3) вероятности).

Кроме вероятности осуществления, важен размер потенциального ущерба. Например, пожары бывают нечасто, но ущерб от каждого из них, как правило, велик. Тяжесть ущерба также можно оценить по трехбалльной шкале.

Оценивая размер ущерба, необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и более отдаленные (подрыв репутации, ослабление позиций на рынке). Оценивая вероятность осуществления угроз, целесообразно исходить не только из среднестатистических данных, но учитывать также специфику конкретных ИС.

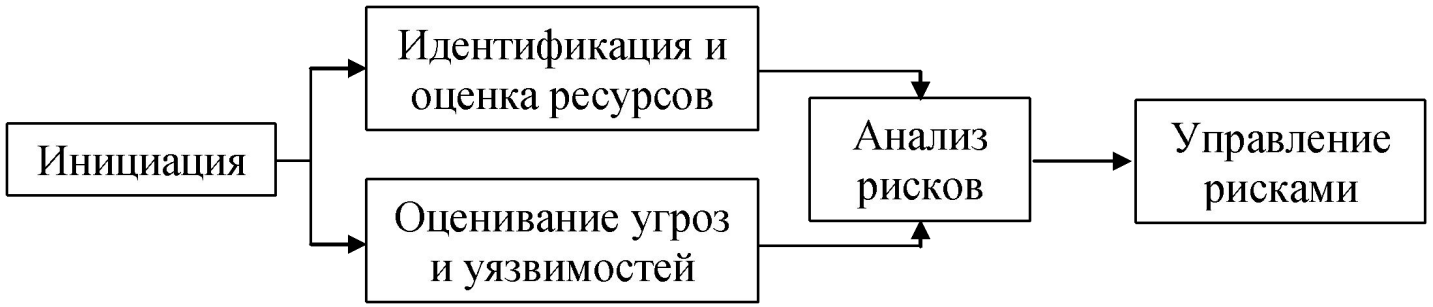
Методика оценки рисков

Одними из достаточно простых методик анализа рисков являются табличные методики. В таблице приведены уровни рисков, соответствующих качественным показателям ресурсов, угроз и уязвимостей.

Показатель (ценность) ресурса	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровни уязвимостей			Уровни уязвимостей			Уровни уязвимостей		
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Наиболее известной методикой анализа и управления рисков является методика CRAMM, состоящая из нескольких этапов:

- ***Инициация*** – формализованное описание границ информационной системы, ее основных функций, категорий пользователей, персонала;
- ***Идентификация и оценка ресурсов*** – описание и определение ценности ресурсов ИС (определяется необходимость полного анализа рисков);
- ***Оценивание угроз и уязвимостей*** – при полном анализе рисков;
- ***Анализ рисков*** – оценивание рисков на основе оценок угроз и уязвимостей или упрощенных методик базового уровня;
- ***Управление рисками*** – поиск адекватных контрмер уменьшения или уклонения от риска.



Этапы и отчетность в методике CRAMM

1 ЭТАП (определение критичности ресурсов):

Модель ресурсов (описание ресурсов и взаимосвязи между ними).

Оценка критичности ресурсов.

Результирующий отчет по первому этапу анализа рисков, в котором суммируются результаты, полученные в ходе обследования.

2 ЭТАП (анализ угроз, уязвимостей, идентификация рисков):

Результаты оценки уровня угроз и уязвимостей.

Результаты оценки величины рисков.

Результирующий отчет по второму этапу анализа рисков.

3 ЭТАП (управление рисками – выбор адекватных контрмер):

Рекомендуемые контрмеры.

Детальная спецификация безопасности.

Оценка стоимости рекомендуемых контрмер.

Список контрмер, отсортированный в соответствии с их приоритетами.

Результирующий отчет по третьему этапу обследования;

Политика безопасности (требования, стратегии и принципы ИБ).

Список мероприятий по обеспечению безопасности.

В табл. приведены значения получаемых качественных оценок рисков.

Вероятность	Ущерб				
	1	2	3	4	5
1	0	1	2	3	4
2	1	2	3	4	5
3	2	3	4	5	6
4	3	4	5	6	7
5	4	5	6	7	8

Для оценки возможного ущерба в методике предлагается использовать следующие критерии:

- ущерб репутации компании;
- нарушение действующего законодательства;
- ущерб для здоровья персонала;
- ущерб, связанный с разглашением информации;
- финансовые потери, связанные с восстановлением ресурсов;
- потери, связанные с невозможностью выполнения обязательств;
- дезорганизация деятельности.