**Тема 10: " МЕТОДЫ И СРЕДСТВА АНАЛИЗА И УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННЫХ СИСТЕМ КОМПАНИЙ"**

***10.1 Обоснование необходимости инвестиций в информационную безопасность компании***

Сегодня не вызывает сомнений необходимость вложений в обеспечение информационной безопасности современного крупного бизнеса. Основной вопрос современного бизнеса - как оценить необходимый уровень вложений в ИБ для обеспечения максимальной эффективности инвестиций в данную сферу. Для решения этого вопроса существует только один способ - применять системы анализа рисков, позволяющие оценить существующие в системе риски и выбрать оптимальный по эффективности вариант защиты (по соотношению существующих в системе рисков к затратам на ИБ).

Для подтверждения факта актуальности задачи обеспечения безопасности бизнеса, рассмотрим для примера отчет ФБР за 2005 год. Данные были собраны на основе опроса 530 американских компаний (средний и крупный бизнес).

Статистика инцидентов области ИТ-секьюрити неумолима. Согласно данным ФБР в 2005 году 56 % опрошенных компаний подвергались атаке.

По статистике, самым большим препятствием на пути принятия каких-либо мер по обеспечению информационной безопасности в компании являются две причины:

1) ограничение бюджета;

2) отсутствие поддержки со стороны руководства.

Обе причины возникают из-за непонимания руководством серьезности вопроса и сложности задачи для ИТ-менеджера обосновать, зачем необходимо вкладывать деньги в информационную безопасность. Часто считается, что основная проблема заключается в том, что ИТ-менеджеры и руководители разговаривают на разных языках - техническом и финансовом, но ведь и самим ИТ-специалистам часто трудно оценить, на что потратить деньги и сколько их требуется для обеспечения большей защищенности системы компании, чтобы эти расходы не оказались напрасными или чрезмерными.

Если ИТ-менеджер четко представляет, сколько компания может потерять денег в случае реализации угроз, какие места в системе наиболее уязвимы, какие меры можно предпринять для повышения уровня защищенности и при этом не потратить лишних денег, и всё это подтверждено документально, то решение задачи убедить руководство обратить внимание и выделить средства на обеспечение информационной безопасности становится значительно более реальным.

Для решения данной задачи были разработаны методики и программные комплексы анализа и контроля информационных рисков.

Среди наиболее распространенных методик анализируются: CRAMM; Microsoft; FRAP; OCTAVE; Risk Watch. Первые две методики рассмотрены ранее. Здесь рассмотрим методики FRAP; OCTAVE; Risk Watch.

Методики FRAP, OCTAVE использует оценку риска на качественном уровне (например, по шкале "высокий", "средний", "низкий"). Количественные методики (риск оценивают через числовое значение, например размер ожидаемых годовых потерь). К этому классу относится методика RiskWatch.

***10.2 Методика FRAP***

Методика "Facilitated Risk Analysis Process (FRAP) (Облегченный Процесс Анализа Риска)" предложена консалтинговой компанией Пелтиер Ассокиетз, специализирующейся на оценке потерь от наличия уязвимых мест в системе безопасности и выработке рекомендаций по их предотвращению. Методика разработана Томасом Пелтиером. В методике, обеспечение ИБ ИС предлагается рассматривать в рамках процесса управления рисками.

**Управление рисками** в сфере ИБ – процесс, позволяющий компаниям найти баланс между затратами средств и сил на средства защиты и получаемым эффектом.

Управление рисками должно начинаться с оценки рисков: должным образом оформленные результаты оценки станут основой для принятия решений в области повышения безопасности системы.

После завершения оценки, проводится анализ соотношения затрат и получаемого эффекта, который позволяет определить те средства защиты, которые нужны, для снижения риска до приемлемого уровня.

Ниже приведены основные этапы оценки рисков. Данный список во многом повторяет аналогичный перечень из других методик, но во FRAP более подробно раскрываются пути получения данных о системе и ее уязвимостях.

**Основные этапы оценки риска**

**1. Определение защищаемых активов**. Производится с использованием опросных листов, изучения документации на систему, использования инструментов автоматизированного анализа (сканирования) сетей.

**2. Идентификация угроз**. При составлении списка угроз могут использоваться разные подходы:

- заранее подготовленные экспертами перечни угроз (checklists), из которых выбираются актуальные для данной системы;

- анализ статистики происшествий в данной ИС и в подобных ей - оценивается частота их возникновения; по ряду угроз, например, угрозе возникновения пожара, подобную статистику можно получить у соответствующих государственных организаций;

- "мозговой штурм", проводимый сотрудниками компании.

**3.** Когда список угроз закончен, каждой из них **сопоставляют вероятность возникновения**. После чего **оценивают ущерб**, который может быть нанесен данной угрозой. Исходя из полученных значений, **оценивается уровень угрозы**.

При проведении анализа, как правило, принимают, что на начальном этапе в системе отсутствуют средства и механизмы защиты. Таким образом оценивается уровень риска для незащищенной ИС, что в последствии позволяет показать эффект от внедрения средств защиты информации (СЗИ).

Оценка производится для вероятности возникновения угрозы и ущерба от нее по следующим шкалам.

**Вероятность** (Probability):

- Высокая (High Probability) - очень вероятно, что угроза реализуется в течение следующего года;

- Средняя (Medium Probability) - возможно угроза реализуется в течение следующего года;

- Низкая (Low Probability) - маловероятно, что угроза реализуется в течение следующего года.

**Ущерб** (Impact) - мера величины потерь или вреда, наносимого активу:

- Высокий (High Impact): остановка критически важных бизнес-подразделений, которая приводит к существенному ущербу для бизнеса, потере имиджа или неполучению существенной прибыли;

- Средний (Medium Impact): кратковременное прерывание работы критических процессов или систем, которое приводит к ограниченным финансовым потерям в одном бизнес-подразделении;

- Низкий (Low Impact): перерыв в работе, не вызывающий ощутимых финансовых потерь.

**Оценка риска** определяется в соответствии с правилом, задаваемым матрицей рисков, изображенной на рис 15. Полученная оценка уровня риска может интерпретироваться следующим образом:

- уровень A - связанные с риском действия (например, внедрение СЗИ) должны быть выполнены немедленно и в обязательном порядке;

- уровень B - связанные с риском действия должны быть предприняты;

- уровень C - требуется мониторинг ситуации (но непосредственных мер по противодействию угрозе принимать, возможно, не надо);

- уровень D -никаких действий в данный момент предпринимать не требуется.



***Рис. 15. Матрица рисков FRAP*** 4.

**4.** После того как угрозы идентифицированы и дана оценка риска, должны быть **определены контрмеры**, позволяющие устранить риск или свести его до приемлемого уровня.

При этом должны приниматься во внимание законодательные ограничения, делающие невозможным или, наоборот, предписывающие в обязательном порядке, использование тех или иных средств и механизмов защиты.

Чтобы определить ожидаемый эффект, можно провести оценку того же риска, но при условии внедрения предлагаемого СЗИ. Если риск снижен недостаточно, возможно, надо применить другое СЗИ.

Вместе с определением средства защиты, надо определить *какие затраты повлечет его приобретение и внедрение* (затраты могут быть как прямые, так и косвенные - см. ниже). Кроме того, необходимо оценить, безопасно ли само это средство, не создает ли оно новых уязвимостей в системе.

Чтобы использовать экономически эффективные средства защиты, нужно проводить анализ соотношения затрат и получаемого эффекта. При этом надо оценивать не только стоимость приобретения решения, но и стоимость поддержания его работы. В затраты могут включаться:

- стоимость реализации проекта, включая дополнительное программное и аппаратное обеспечение;

- снижение эффективности выполнения системой своих основных задач;

- внедрение дополнительных политик и процедур для поддержания средства;

- затраты на найм дополнительного персонала или переобучение имеющегося.

**5. Документирование**. Когда оценка рисков закончена, ее результаты должны быть подробно документированы в стандартизованном формате. Полученный отчет может быть использован при определении политик, процедур, бюджета безопасности и т.д.

***10.3 Методика OCTAVE***

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – методика поведения оценки рисков в организации. Разработана Инженерным Институтом Программного Обеспечения (SEI) при университете Карнеги Меллон (университет и исследовательский центр, расположенный в Питтсбурге, штат Пенсильвания, США).

Особенность данной методики заключается в том, что весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов. Для этого создается смешанная группа, включающая как технических специалистов, так и руководителей разного уровня, что позволяет всесторонне оценить последствия для бизнеса возможных инцидентов в области безопасности и разработать контрмеры.

OCTAVE предполагает три фазы анализа:

1. разработка профиля угроз, связанных с активом;

2. идентификация инфраструктурных уязвимостей;

3. разработка стратегии и планов безопасности.

**Профиль угрозы** включает в себя указания на актив (asset), тип доступа к активу (access), источник угрозы (actor), тип нарушения или мотив (motive), результат (outcome) и ссылки на описания угрозы в общедоступных каталогах. По типу источника, угрозы в OCTAVE делятся на:

1. угрозы, исходящие от человека-нарушителя, действующего через сеть передачи данных;

2. угрозы, исходящие от человека-нарушителя, использующего физический доступ;

3. угрозы, связанные со сбоями в работе системы;

4. прочие.

Результатом может быть раскрытие (disclosure), изменение (modification), потеря или разрушение (loss/destruction) информационного ресурса или разрыв подключения. Отказ в обслуживании (interruption).

Методика OCTAVE предлагает при описании профиля использовать "деревья вариантов", пример подобного дерева для угроз класса 1) приведен на Рис.16. При создании профиля угроз рекомендуется избегать обилия технических деталей – это задача второго этапа исследования. Главная задача первой стадии – стандартизованным образом описать сочетание угрозы и ресурса.

Предположим, что на предприятии имеется информационный ресурс (актив) – база данных (БД) отдела кадров (HR Database). Профиль, соответствующий угрозе кражи информации сотрудником предприятия представлен в таблице 1.

*Таблица 1. Пример профиля угрозы.*

|  |  |
| --- | --- |
| Ресурс (*Asset*) | БД отдела кадров (*HR Database*) |
| Тип доступа (*Access*) | Через сеть передачи данных (*Network*) |
| Источник угрозы (*Actor*) | Внутренний (*Inside*) |
| Тип нарушения (*Motive*) | Преднамеренное (*Deliberate*) |
| Уязвимость (*Vulnerability)* | - |
| Результат (*Outcome*) | Раскрытие данных (Disclosure) |
| Ссылка на каталог уязвимостей (*Catalog reference*) | - |



***Рис. 16 Дерево вариантов, использующееся при описании профиля.***

Вторая фаза исследования системы в соответствии с методикой – **идентификация инфраструктурных уязвимостей.** В ходе этой фазы определяется инфраструктура, поддерживающая существование выделенного ранее актива.

Например, если это БД отдела кадров, то нам для работы с ней нужен сервер, на котором база размещена, рабочая станция служащего отдела кадров и то окружение, которое может позволить получить к ней доступ (например, соответствующий сегмент локальной сети).

Рассматриваются компоненты следующих классов: серверы; сетевое оборудование; СЗИ; персональные компьютеры; домашние персональные компьютеры "надомных" пользователей, работающих удаленно, но имеющих доступ в сеть организации; мобильные компьютеры; системы хранения; беспроводные устройства; прочее.

Группа, проводящая анализ для каждого сегмента сети, отмечает, какие компоненты в нем проверяются на наличие уязвимостей. Уязвимости проверяются сканерами безопасности уровня операционной системы, сетевыми сканерами безопасности, специализированными сканерами (для конкретных web-серверов, СУБД и проч.), с помощью списков уязвимостей (checklists), тестовых скриптов.

Для каждого компонента определяется:

- список уязвимостей, которые надо устранить немедленно (high-severity vulnerabilities);

- список уязвимостей, которые надо устранить в ближайшее время (middle-severity vulnerabilities);

- список уязвимостей, в отношении которых не требуется немедленных действий (low-severity vulnerabilities).

По результатам стадии готовится отчет, в котором указывается, какие уязвимости обнаружены, какое влияние они могут оказать на выделенные ранее активы, какие меры надо предпринять для устранения уязвимостей.

**Разработка стратегии и планов безопасности** – третья стадия исследования системы. Она начинается с оценки рисков, которая проводится на базе отчетов по двум предыдущим этапам.

В OCTAVE *при оценке риска дается только оценка ожидаемого ущерба, без оценки вероятности*. Шк**ала: высокий (high), средний (middle), низкий (low).** Оценивается финансовый ущерб, ущерб репутации компании, жизни и здоровью клиентов и сотрудников, ущерб, который может вызвать судебное преследование в результате того или иного инцидента. Описываются значения, соответствующие каждой градации шкалы (например, для малого предприятия финансовый ущерб в $10000 – высокий, для более крупного - средний).

**Далее, разрабатывают планы снижения рисков нескольких типов**:

- долговременные;

- на среднюю перспективу;

- списки задач на ближайшее время.

Для определения мер противодействия угрозам в методике предлагаются каталоги средств. Хотелось бы еще раз подчеркнуть, что в отличие от прочих методик, OCTAVE не предполагает привлечения для исследования безопасности ИС сторонних экспертов, а вся документация по OCTAVE общедоступна и бесплатна, что делает методику особенно привлекательной для предприятий с жестко ограниченным бюджетом, выделяемым на цели обеспечения ИБ

***10.4 Методика RiskWatch***

Компания RiskWatch разработала собственную методику анализа рисков и семейство программных средств, в которых она в той либо иной мере реализуется.

В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности:

- RiskWatch for Physical Security – для анализа физической защиты ИС;

- RiskWatch for Information Systems – для информационных рисков;

- HIPAA-WATCH for Healthcare Industry – для оценки соответствия требованиям стандарта HIPAA (US Healthcare Insurance Portability and Accountability Act), актуальных в основном для медицинских учреждений, работающих на территории США;

- RiskWatch RW17799 for ISO 17799 – для оценки соответствия ИС требованиям стандарта международного стандарта ISO 17799.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются **ожидаемые годовые потери** (Annual Loss Expectancy, ALE) и **оценка возврата инвестиций** (Return on Investment, ROI).

RiskWatch ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. В основе продукта RiskWatch находится методика анализа рисков, которая состоит из четырех этапов.

**Первый этап – определение предмета исследования**. Здесь описываются такие параметры, как тип организации, состав исследуемой системы (в общих чертах), базовые требования в области безопасности.

Для облегчения работы аналитика, в шаблонах, соответствующих типу организации ("коммерческая информационная система", "государственная/военная информационная система" и т.д.), есть списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты. Из них нужно выбрать те, что реально присутствуют в организации.

Например, категории потерь:

- Задержки и отказ в обслуживании;

- Раскрытие информации;

- Прямые потери (например, от уничтожения оборудования огнем);

- Жизнь и здоровье (персонала, заказчиков и т.д.);

- Изменение данных;

- Косвенные потери (например, затраты на восстановление);

- Репутация.

**Второй этап – ввод данных, описывающих конкретные характеристики системы**. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей. На этом этапе, в частности, подробно описываются ресурсы, потери и классы инцидентов. Классы инцидентов получаются путем сопоставления категории потерь и категории ресурсов.

Для выявления возможных уязвимостей используется вопросник, база которого содержит более 600 вопросов. Вопросы связаны с категориями ресурсов.

Также задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Если для выбранного класса угроз в системе есть среднегодовые оценки возникновения (LAFE и SAFE), то используются они. Все это используется в дальнейшем для расчета эффекта от внедрения средств защиты.



***Рис. 17 Определение категорий защищаемых ресурсов***

**Третий этап - количественная оценка риска**. На этом этапе рассчитывается профиль рисков, и выбираются меры обеспечения безопасности. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих шагах исследования. По сути, риск оценивается с помощью математического ожидания потерь за год. Например, если стоимость сервера $150000, а вероятность того, что он будет уничтожен пожаром в течение года, равна 0.01, то ожидаемые потери составят $1500.

Формула расчета (**m=p\*v**, где m – математическое ожидание, p – вероятность возникновения угрозы, v – стоимость ресурса) претерпела некоторые изменения, в связи с тем, что RiskWatch использует определенные американским институтом стандартов NIST оценки, называемые LAFE и SAFE.

LAFE (Local Annual Frequency Estimate) – показывает, сколько раз в год в среднем данная угроза реализуется в данном месте (например, в городе). SAFE (Standard Annual Frequency Estimate) - показывает, сколько раз в год в среднем данная угроза реализуется в этой "части мира" (например, в Северной Америке). Вводится также поправочный коэффициент, который позволяет учесть, что в результате реализации угрозы защищаемый ресурс может быть уничтожен не полностью, а только частично.

Формулы (1) и (2) показывают варианты расчета показателя ALE:

**ALE= Asset Value x Exposure Factor x Frequency (1)**

где:

* Asset Value - стоимость рассматриваемого актива (данных, программ, аппаратуры и т.д.);
* Exposure Factor - коэффициент воздействия - показывает, какая часть (в процентах) от стоимости актива, подвергается риску;
* Frequency - частота возникновения нежелательного события;
* ALE - это оценка ожидаемых годовых потерь для одного конкретного актива от реализации одной угрозы.

Когда все активы и воздействия идентифицированы и собраны вместе, то появляется возможность оценить общий риск для ИС, как сумму всех частных значений.

Можно ввести показатели "ожидаемая годовая частота происшествия" (Annualized Rate of Occurrence – ARO) и "ожидаемый единичный ущерб" (Single Loss Expectancy – SLE), который может рассчитываться как разница первоначальной стоимости актива и его остаточной стоимости после происшествия (хотя подобный способ оценки применим не во всех случаях, например, он не подходит для оценки рисков, связанных с нарушением конфиденциальности информации). Тогда, для отдельно взятого сочетания угроза-ресурс применима формула (2).

**ALE= ARO x SLE (2)**

Дополнительно рассматриваются сценарии "что если:", которые позволяют описать аналогичные ситуации при условии внедрения средств защиты. Сравнивая ожидаемые потери при условии внедрения защитных мер и без них можно оценить эффект от таких мероприятий.

 RiskWatch включает в себя базы с оценками LAFE и SAFE, а также с обобщенным описанием различных типов средств защиты.

Эффект от внедрения средств защиты количественно описывается с помощью показателя ROI (Return on Investment – возврат инвестиций), который показывает отдачу от сделанных инвестиций за определенный период времени. Рассчитывается он по формуле:

 **(3)**

где:

- Costsj – затраты на внедрение и поддержание j-меры защиты;

- Benefitsi – оценка той пользы (т.е. ожидаемого снижения потерь), которую приносит внедрение данной меры защиты;

- NPV (Net Present Value) – чистая текущая стоимость.

**Четвертый этап - генерация отчетов**.

- Типы отчетов:

- Краткие итоги.

- Полные и краткие отчеты об элементах, описанных на стадиях 1 и 2.

- Отчет от стоимости защищаемых ресурсов и ожидаемых потерях от реализации угроз.

- Отчет об угрозах и мерах противодействия.

- Отчет о ROI (фрагмент – на рис. 18).

- Отчет о результатах аудита безопасности.



***Рис. 18 Пример графика показателя ROI для различных мер защиты***

Таким образом, рассматриваемое средство позволяет оценить не только те риски, которые сейчас существуют у предприятия, но и ту выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты.

Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия.

Для отечественных пользователей проблема заключается в том, что получить используемые в RiskWatch оценки (такие как LAFE и SAFE) для наших условий достаточно проблематично. Хотя сама методология может с успехом применяться и у нас.

Подводя итог, можно отметить, что конкретную методику проведения анализа рисков на предприятии и инструментальные средства, поддерживающие ее, нужно выбирать, учитывая следующие факторы:

* Наличие экспертов, способных дать достоверные оценки объема потерь от угроз информационной безопасности;
* Наличие на предприятии достоверной статистки по инцидентам в сфере информационной безопасности;
* Нужна ли точная количественная оценка последствий реализации угроз или достаточно оценки на качественном уровне.

К недостаткам RiskWatch можно отнести:

Такой метод подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов.

Полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывает понимание риска с системных позиций – метод не учитывает комплексный подход к информационной безопасности.

Программное обеспечение RiskWatch существует только на английском языке.

Высокая стоимость лицензии (от 10000 долл. за одно рабочее место для небольшой компании).