**Лекция 5 (Продолжение)**

**Анализ и управление рисками при реализации информационной безопасности**

Одним из важнейших аспектов реализации политики ИБ является анализ угроз, оценка их достоверности и тяжести вероятных последствий. Реально риск появляется там, где есть вероятность осуществления угрозы, при этом величина риска прямо пропорциональна величине этой вероятности ([рис. 4.11](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=3#image.4.11)).

Суть деятельности по управлению рисками состоит в том, чтобы оценить их размер, выработать меры по уменьшению и создать механизм контроля того, что остаточные риски не выходят за приемлемые ограничения. Таким образом, управление рисками включает в себя два вида деятельности: оценка рисков и выбор эффективных и экономичных защитных и регулирующих механизмов. Процесс управления рисками можно подразделить на следующие этапы [Галатенко В. А., 2006]:

* идентификация активов и ценности ресурсов, нуждающихся в защите;
* выбор анализируемых объектов и степени детальности их рассмотрения;
* анализ угроз и их последствий, определение слабостей в защите;
* классификация рисков, выбор методологии оценки рисков и проведение оценки;
* выбор, реализация и проверка защитных мер;
* оценка остаточного риска.



**Рис. 4.11.**Неопредленнось как основа формирования риска

Политика ИБ включает разработку стратегии управления рисками разных классов.

Краткий перечень наиболее распространенных угроз приводился выше (см. п. 17.2). Целесообразно выявлять не только сами угрозы, но и источники их возникновения — это поможет правильно оценить риск и выбрать соответствующие меры нейтрализации. Например, нелегальный вход в систему повышает риск подбора пароля или подключения к сети неавторизованного пользователя или оборудования.

Очевидно, что для противодействия каждому способу нелегального входа нужны свои механизмы безопасности. После идентификации угрозы необходимо оценить вероятность ее осуществления и размер потенциального ущерба.

Оценивая тяжесть ущерба, необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и более отдаленные, в частности подрыв репутации компании, ослабление её позиций на рынке и т. п.

После проведения идентификации и анализа угроз, их возможных последствий имеется несколько подходов к управлению: оценка риска, уменьшение риска, уклонение от риска, изменение характера риска, принятие риска, выработка корректирующих мероприятий ([рис. 4.12](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=3#image.4.12)).



**Рис. 4.12.**Схема управления рисками

При идентификации активов и информационных ресурсов — тех ценностей, которые нужно защитить — следует учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, в том числе текущий рейтинг и репутацию компании. Тем не менее, одним из главных результатов процесса идентификации активов является получение детальной информационной структуры организации и способов ее использования.

Выбор анализируемых объектов и степень детальности их рассмотрения — следующий шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру, для крупной — следует сосредоточиться на наиболее важных (критичных) сервисах. Если важных сервисов много, то выбираются те из них, риски для которых заведомо велики или неизвестны. Если информационной основой организации является локальная сеть, то в число аппаратных объектов следует включить компьютеры, периферийные устройства, внешние интерфейсы, кабельное хозяйство и активное сетевое оборудование.

К программным объектам следует отнести операционные системы (сетевая, серверные и клиентские), прикладное программное обеспечение, инструментальные средства, программы управления сетью и отдельными подсистемами. Важно зафиксировать в каких узлах сети хранится программное обеспечение, где и как используется. Третьим видом информационных объектов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, а также способы доступа к ним. Все это важно для оценки рисков и последствий нарушений информационной безопасности.

Оценка рисков производится на основе накопленных исходных данных и оценки степени определенности угроз. Вполне допустимо применить такой простой метод, как умножение вероятности осуществления угрозы на величину предполагаемого ущерба. 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. По этой шкале можно оценивать приемлемость рисков.

Если какие-либо риски оказались недопустимо высокими, необходимо реализовать дополнительные защитные меры. Для ликвидации или уменьшения слабости, сделавшей опасную угрозу реальной, можно применять несколько механизмов безопасности, отличающихся эффективностью и невысокой стоимостью. Например, если велика вероятность нелегального входа в систему, можно ввести длинные пароли, задействовать программу генерации паролей или закупить интегрированную систему аутентификации на основе интеллектуальных карт. Если имеется вероятность умышленного повреждения серверов различного назначения, что грозит серьезными последствиями, можно ограничить физический доступ персонала в серверные помещения и усилить их охрану.

Технология оценки рисков должна сочетать формальные метрики и формирование реальных количественных показателей для оценки. С их помощью необходимо ответить на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства экономически выгодно использовать.



**Рис. 4.13.**Схема оценки и снижения рисков

Методология снижения рисков. Многие риски можно существенно уменьшить путем использования простых и недорогих контрмер. Например, грамотное (регламентированное) управление доступом снижает риск несанкционированного вторжения. От некоторых классов рисков можно уклониться — вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов. Некоторые риски не могут быть уменьшены до малой величины, однако после реализации стандартного набора контрмер их можно принять, постоянно контролируя остаточную величину риска ([рис. 4.13](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=3#image.4.13)).

Оценка стоимости защитных мер должна учитывать не только прямые расходы на закупку оборудования и/или программного обеспечения, но и расходы на внедрение новинки, обучение и переподготовку персонала. Эту стоимость можно выразить в некоторой шкале и затем сопоставить ее с разностью между вычисленным и приемлемым риском. Если по этому показателю средство защиты оказывается экономически выгодным, его можно принять к дальнейшему рассмотрению.



**Рис. 4.14.**Итерационный процесс управления рисками

Контроль остаточных рисков в обязательном порядке включается в текущий контроль системы ИБ. Когда намеченные меры приняты, необходимо проверить их действенность — убедиться, что остаточные риски стали приемлемыми. В случае систематического повышения остаточных рисков необходимо проанализировать допущенные ошибки и немедленно принять корректирующие меры.

Управление рисками является многоступенчатым итерационным процессом ([рис. 4.14](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=3#image.4.14)).

Практически все его этапы связаны между собой, и по завершении почти любого из них может выявиться необходимость возврата к предыдущему. Так, при идентификации активов может возникнуть понимание, что выбранные границы анализа следует расширить, а степень детализации — увеличить. Особенно труден первичный анализ, когда многократные возвраты к началу неизбежны. Управление рисками — типичная оптимизационная задача, принципиальная трудность состоит в её грамотной постановке на уровне высшего менеджмента, сочетании оптимальных методик и описания исходных данных ([рис. 4.15](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=3#image.4.15)).



**Рис. 4.15.**Формирование деятельности по управлению ИТ-рисками

Методологии "Оценка рисков" (Risk Assessment) и "Управление рисками" (Risk Management) стали неотъемлемой составляющей деятельности в области обеспечения непрерывности бизнеса (Business Continuity) и информационной безопасности (Information Security). Программа реализации ИБ и наборы политик базируются на совокупности системных действий и практических шагов ([рис. 4.16](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=3#image.4.16)-[рис. 4.19](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=3#image.4.19)).



**Рис. 4.16.**Совокупности системных действий и практических шагов (1)



**Рис. 4.17.**Совокупности системных действий и практических шагов (2)



**Рис. 4.18.**Совокупности системных действий и практических шагов (3)



**Рис. 4.19.**Совокупности системных действий и практических шагов (4)

Подготовлено и активно используются более десятка различных международных стандартов и спецификаций, детально регламентирующих процедуры управления информационными рисками: ISO 15408: 1999 ("Common Criteria for Information Technology Security Evaluation"), ISO 17799:2002 ("Code of Practice for Information Security Management"), NIST 80030, SAS 78/94, COBIT.

Методика и инструментальное средство RA Software Tool основаны на требованиях международных стандартов ISO 17999 и ISO 13335 (части 3 и 4), а также на требованиях руководств Британского национального института стандартов (BSI) — PD 3002 ("Руководство по оценке и управлению рисками"), PD 3003 ("Оценка готовности компании к аудиту в соответствии с BS 7799"), PD 3005 ("Руководство по выбору системы защиты").

На практике такие методики управления рисками позволяют:

* создавать модели информационных активов компании с точки зрения безопасности;
* классифицировать и оценивать ценности активов;
* составлять списки наиболее значимых угроз и уязвимостей безопасности;
* ранжировать угрозы и уязвимости безопасности;
* оценивать и отрабатывать риски;
* разрабатывать корректирующие меры;
* обосновывать средства и меры контроля рисков;
* оценивать эффективность/стоимость различных вариантов защиты;
* формализовать и автоматизировать процедуры оценивания и управления рисками.

Отработка рисков включает в себя ряд важных этапов, которые в обязательном порядке включаются в плановую работу по обеспечению информационной безопасности ([рис. 4.20](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=3#image.4.20)).

Применение соответствующих программных средств позволяет уменьшить трудоемкость проведения анализа рисков и выбора контрмер. В настоящее время разработано более десятка программных продуктов для анализа и управления рисками базового уровня безопасности. Примером достаточно простого средства является программный пакет BSS (Baseline Security Survey, UK).

Программные продукты более высокого класса: CRAMM (компания Insight Consulting Limited, UK), Risk Watch, COBRA (Consultative Objective and Bi-Functional Risk Analysis), Buddy System. Наиболее популярный из них — CRAMM (Complex Risk Analysis and Management Method), реализующий метод анализа и контроля рисков. Существенным достоинством метода является возможность проведения детального исследования в сжатые сроки с полным документированием результатов.



**Рис. 4.20.**Этапы отработки риска

В основе методов, подобных CRAMM, лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Метод является универсальным и подходит как для больших, так и для мелких организаций, как правительственного, так и коммерческого сектора.

К сильным сторонам метода CRAMM относится следующее:

* CRAMM является хорошо структурированным и широко опробованным методом анализа рисков, позволяющим получать реальные практические результаты;
* программный инструментарий CRAMM может использоваться на всех стадиях проведения аудита безопасности ИС;
* в основе программного продукта лежит достаточно объемная база знаний по контрмерам в области информационной безопасности, базирующаяся на рекомендациях стандарта BS 7799;
* гибкость и универсальность метода CRAMM позволяет использовать его для аудита ИС любого уровня сложности и назначения;
* CRAMM можно использовать в качестве инструмента для разработки плана непрерывности бизнеса и политик информационной безопасности организации;
* CRAMM может использоваться в качестве средства документирования механизмов безопасности ИС.

Для коммерческих организаций имеется коммерческий профиль стандартов безопасности (Commercial Profile), для правительственных организаций — правительственный (Government Profile). Правительственный вариант профиля, также позволяет проводить аудит на соответствие требованиям американского стандарта TCSEC ("Оранжевая книга").