ОСНОВНЫЕ ПОДХОДЫ К АНАЛИЗУ И ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.Н. Максименко, *доцент кафедры «Информационная безопасность и автоматизация» МТУСИ, vladmaks@yandex.ru;*
Е.В. Ясюк, *аспирант МТУСИ, jusjuk@rambler.ru*

УДК 004

Аннотация. При построении системы информационной безопасности разработчики сталкиваются с проблемой определения необходимого уровня обеспечения доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры. Для поиска «границ» безопасности информационной системы можно использовать определенные стандарты и регламенты в сфере информационной безопасности, однако они не всегда там четко определяются. Поэтому используются определенные методики управления рисков, которые позволяют идентифицировать риски, ранжировать их по степени опасности, по вероятности возникновения, а также выработать определенный метод обработки данных рисков.

В статье описывается предназначение систем анализа и оценки рисков, рассматриваются вопросы необходимости и причин возникновения такого рода систем, приводятся и сравниваются основные подходы к решению проблемы управления рисками, а также описываются и сравниваются существующие программные средства, в которых применяются данные подходы.

Ключевые слова: аудит информационной безопасности; риски информационной безопасности; угроза информационной безопасности; защита информации, управление рисками.

MAIN APPROACHES TO THE ANALYSIS AND ESTIMATION OF RISKS OF INFORMATION SECURITY

Vladimir Maksimenko, *associate professor "Information security and automation" of MTUCI;*
Yegor Yasyuk, *graduate student of MTUCI*

Annotation. When constructing the system of ensuring information security developers are faced with the problem of determining the required level of availability, integrity and confidentiality of information resources and supporting infrastructure. To search for "borders" of the information system security certain standards and regulations in the field of information security can be used, but they are not always clearly defined. Certain methods of risk management are used to identify risks, rank them by severity, likelihood of occurrence, and to develop a method for the treatment of these risks.

The article describes the purpose of systems analysis and risk assessment, discusses the necessity and the reasons for the emergence of such systems, describes and compares the main approaches to the problem of risk management and describes and compares existing software tools that utilize these approaches.

Keywords: audit of information security; information security risk; information security threat; information protection, risk management.

Введение

Зачем нужно исследовать риски в сфере информационной безопасности (ИБ) и что это может дать при разработке системы обеспечения ИБ для информационной системы (ИС)?

Для любого проекта, требующего финансовых затрат на его реализацию, весьма желательно уже на начальной стадии определить, что мы будет считать признаком завершения

работы и как будем оценивать результаты проекта. Для задач, связанных с обеспечением ИБ это более чем актуально. Ведь затраты на обеспечение высокого уровня безопасности могут быть неоправданными. Фактически встает вопрос: какой уровень защиты должен быть у рассматриваемой системы? Для ответа на данный вопрос в процессе создания системы ИБ можно использовать два подхода.

Первый ориентируется на основные стандарты в сфере ИБ (например, [1]) или какой-либо другой набор требований. Тогда критерий достижения цели в области безопасности – это выполнение заданного набора требований. Критерий эффективности – минимальные суммарные затраты на выполнение поставленных функциональных требований. Однако требуемый уровень защищенности в данных документах не всегда строго определен, поэтому определить эффективный уровень защищенности ИС достаточно сложно.

Второй подход связан с оценкой и управлением рисками. Изначально он произошел из принципа «разумной достаточности» примененного к сфере обеспечения ИБ. Этот принцип описывается набором утверждений:

- абсолютно непреодолимой защиты создать невозможно;
- необходимо соблюдать баланс между затратами на защиту и получаемым эффектом;
- стоимость средств защиты не должна превышать стоимости защищаемой информации;
- затраты нарушителя на несанкционированный доступ к информации должны превышать тот эффект, который он получит, осуществив подобный доступ.

Риском в сфере ИБ называется потенциальная возможность понести убытки из-за нарушения безопасности информационной системы (ИС).

Наиболее подробно процесс анализа рисков описывается в [2]. При анализе рисков рассматривается ИС в ее исходном состоянии, оценивается размер ожидаемых потерь от инцидентов, связанных с информационной безопасностью за определенный период. После этого, делается оценка того, как предлагаемые средства и меры обеспечения безопасности влияют на снижение рисков, и сколько они стоят.

«Зачатки» идеи управления рисков возникли еще в 70-х гг., когда была разработана модель безопасности с полным перекрытием (или модель Клементса-Хоффмана [3]).

Модель Клементса-Хоффмана

В своем первоначальном виде модель Клементса-Хоффмана была очень «идеализирована», однако именно в процессе анализа данной модели и возникла проблема необходимости оценки угроз.

Модель строится исходя из постулата, что система безопасности должна иметь, по крайней мере, одно средство для обеспечения безопасности на каждом возможном пути воздействия нарушителя на ИС.

Для описания системы защиты информации с полным перекрытием рассматриваются три множества [3]:

- множество угроз $U = \{U_i\}, i = \overline{1,m}$;
- множество объектов защиты $O = \{O_j\}, j = \overline{1,n}$;
- множество механизмов защиты $M = \{M_k\}, k = \overline{1,r}$.

Элементы множеств U и O находятся между собой в отношениях «угроза – объект», определяемых двухдольным графом, который изображен на рисунке 1. Дуга $<U_i, O_j>$ существует тогда, когда U_i – средство получения доступа к объекту O_j.

На рис. 1 показан двудольный граф «угроза – объект».

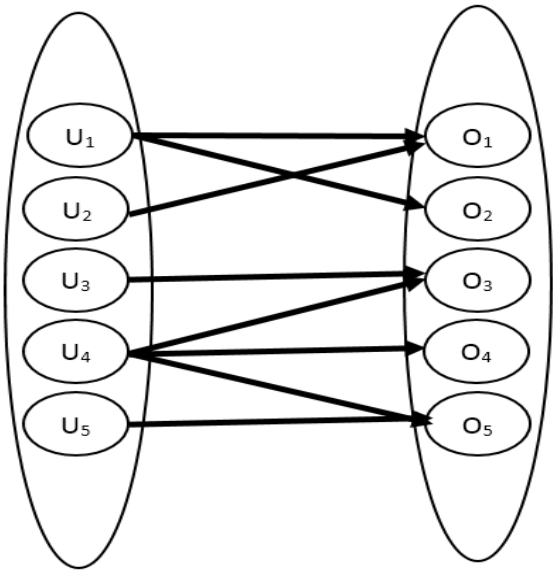

Рисунок 1.

Следует отметить, что связь между угрозами и объектами необязательно должна быть связью типа «один к одному» – угроза может распространяться на любое число объектов, а объект может быть уязвим со стороны более чем одной угрозы.

Цель защиты состоит в том, чтобы перекрыть каждую дугу графа и воздвигнуть барьер для доступа на этом пути. Общая постановка задачи формулируется в следующем виде: множество средств защиты информации M обеспечивает защиту множества объектов O от множества угроз U. В идеале каждое средство mk должно характеризовать некоторое ребро $<U_i, O_j>$ из указанного графа.

Применение множества средств защиты M преобразует двудольный граф в трехдольный (рис. 2).

На рис. 2 показан трехдольный граф «угроза – средство безопасности – объект».

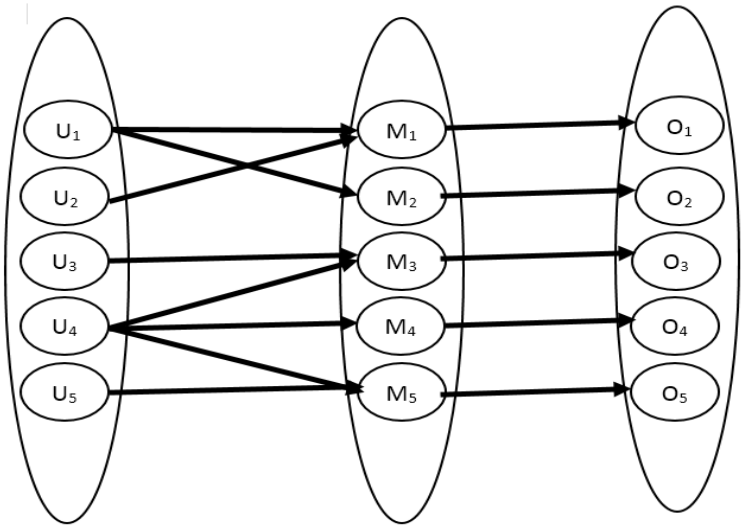

Рисунок 2.

В защищенной системе все ребра представляются в виде $<U_i, M_k>$ и $<M_k, O_j>$. При этом одно и то же средство защиты может перекрывать более одной угрозы и защищать более одного объекта.

Вводится понятие «система с полным перекрытием» – это система, в которой имеются средства защиты на каждый возможный путь проникновения.

Развитие этой модели предполагает введение еще двух элементов [4]:

- V – набор уязвимых мест, определяемый подмножеством декартова произведения U×O. Под уязвимостью системы защиты будет пониматься возможность осуществления угрозы U_i в отношении объекта O_j;
- B – набор барьеров, определяемый декартовым произведением V×M. Барьеры – это пути осуществления угроз безопасности, перекрытые средствами защиты.

Получаем пятидольный граф. На рис. 3 показан пятидольный граф «угроза – средство безопасности – барьер – уязвимость – объект».

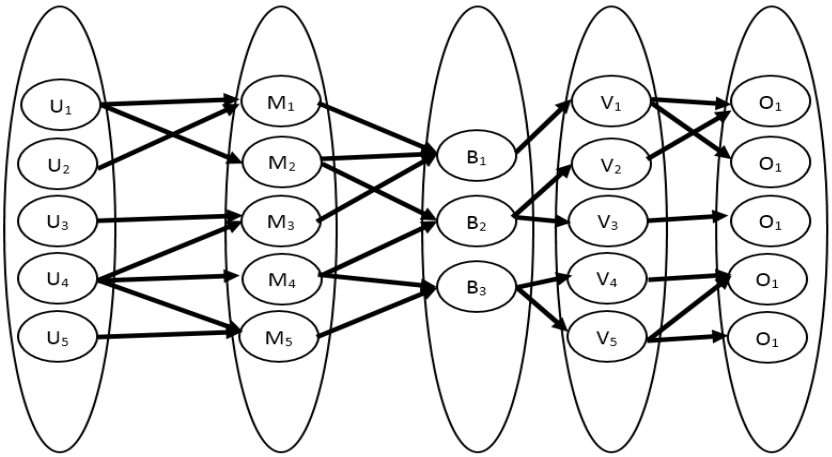

Рисунок 3.

Теперь, если каждой дуге графа поставить в соответствие весовой коэффициент, то имеется возможность количественно определить степень защиты системы.

Отметим, что данная модель носит «утопический» характер. В ней не учитывается стоимость внедряемых средств зашиты, а также соотношение этой стоимости к возможным потерям при реализации конкретной угрозы. Учитывая, что у нас всегда существуют не только как материальные, так и временные ограничения при создании системы обеспечения ИБ, построить систему с полным перекрытием не представляется возможным.

Также поиск всех возможных воздействий злоумышленника на объект зачастую не может быть выполнен. Ведь помимо известных способов осуществления угрозы в будущем могут возникнуть и новые.

Таким образом, если обеспечить защиту абсолютно от всех угроз невозможно, значит встает вопрос выбора тех угроз, от которых мы будем защищать систему.

Наконец, каждый барьер защиты в реальности обеспечивает лишь некоторую степень сопротивляемости угрозам безопасности. Прочность барьера характеризуется величиной остаточного риска R_i ([4]), который определяется по формуле 1:

$$R_i = P_i * Q_i * (1 - P_q) \quad (1)$$

где: P_i – вероятность появления угрозы U_i; Q_j – величина ущерба при удачном осуществлении угрозы U_i в отношении защищаемого объекта O_j; P_q – степень сопротивляемости барьера B_q, характеризующаяся вероятностью его преодоления.

Именно здесь мы сталкиваемся с необходимостью анализа степени защиты объекта от определенной угрозы. Так как от угрозы риска возникновения угрозы полностью избавиться нельзя, предлагаются определенные способы обработки риска (снижение, устранение, перенос или принятие).

Таким образом, при построении системы информационной безопасности встает проблема определения степени защиты от существующих угроз безопасности. Для этого нам необходимо определенным образом ранжировать угрозы в зависимости от степени опасности и выработать меры по их обработке.

Современные методики управления рисками

В процессе решения изложенной выше проблемы было создано множество систем управления рисков. Задача каждой из них заключается в оценке рисков ИС по различным параметрам (возможный ущерб, вероятность возникновения угрозы, тяжесть последствий и др.) и выработке рекомендаций по обработке риска.

Несмотря на повышение интереса к управлению рисками, используемые в настоящее время методики относительно неэффективны, поскольку этот процесс во многих компаниях осуществляется каждым подразделением независимо. Централизованный контроль над их действиями зачастую отсутствует, что исключает возможность реализации единого и целостного подхода к управлению рисками во всей организации.

Все известные методики оценки и анализа рисков можно разделить на [5]:

- методики, использующие оценку риска на качественном уровне (например, по шкале «высокий», «средний», «низкий»);
- количественные методики (риск оценивается через числовое значение, например, размер ожидаемых годовых потерь);
- методики, использующие смешанные оценки.

При качественной оценке риска определяют последствия, вероятность и уровень риска по экспертным шкалам; оценка последствий и вероятности может быть объединена; сравнительную оценку уровня риска в этом случае проводят в соответствии с качественными критериями. Преимущество качественного анализа состоит в том, что он позволяет быстро и относительно «дешево» (с минимальными затратами ресурсов) определить максимально возможное количество факторов и областей, в которых возможно явное или неявное проявление рисков. При использовании только качественного подхода мы проанализируем причины возникновения рисков, последствия при их реализации, однако используемая шкала оценки носит субъективный характер, также могут возникнуть сложности в сравнении угроз одной категории.

При количественном анализе оценивают практическую значимость и стоимость последствий, их вероятности, и получают значение уровня риска в определенных единицах. Полный количественный анализ не всегда может быть возможен. В таком случае ранжирование рисков высококвалифицированными специалистами (экспертами) может быть более эффективно. В процессе количественного анализа происходит сравнение и более качественная приоритезация и переопритезация рисков. Использование только количественного подхода позволяет более точно (численно) сравнивать риски, однако мы не учитываем причины их возникновения, последствия.

Поэтому при анализе информационных систем, учитывая их сложность, желательно применять смешанный подход, который использует как качественную, так и количественную шкалы оценок. Это обеспечит наиболее всесторонний и комплексный подход к решению задачи управления рисками.

Программные продукты для управления рисками

Рассмотрим основные системы анализа и оценки рисков (подробнее в [6-7]):

- ***Оценка CRAMM (смешанный подход)***

Данная методика не учитывает сопроводительной документации, такой как описание бизнес-процессов или отчетов по проведенным оценкам рисков. В отношении стратегии работы с рисками CRAMM предполагает использование только методов их снижения. В методике отсутствуют: процесс интеграции способов управления, мониторинг эффективности используемых способов управления и способов управления остаточными рисками, процесс реагирования на инциденты.

Минусами CRAMM является и необходимость привлечения специалистов высокой квалификации, трудоемкость и длительность процесса оценки рисков. Кроме того, следует отметить высокую стоимость лицензии.

- ***Оценка ГРИФ (смешанный подход)***

Методика ГРИФ использует количественные и качественные способы оценки рисков, а также определяет условия, при которых последние могут быть приняты компанией, включает в себя расчет возврата инвестиций на внедрение мер безопасности. В отличие от других методик анализа рисков, ГРИФ предлагает все способы снижения рисков (обход, снижение и принятие). Данная методика учитывает сопроводительную документацию (описание бизнес-процессов или отчетов по проведенным оценкам рисков ИБ).

- ***Оценка RiskWatch (количественный подход)***

Трудоемкость работ по анализу рисков с использованием этого метода сравнительно невелика. Существенным достоинством RiskWatch является интуитивно понятный интерфейс и большая гибкость метода, обеспечиваемая возможностью введения новых категорий, описаний, вопросов и т. д.

Недостатки: анализ рисков проводится только на программно-техническом уровне, не учитываются административные и организационные факторы, очень высокая стоимость [8-10].

- ***Оценка CORAS (качественный подход)***

Недостаток CORAS в том, что в нем не предусмотрена периодичность проведения оценки рисков и обновление их величин, что свидетельствует о том, что методика пригодна для выполнения разовых оценок и не годится для регулярного использования.

Положительной стороной CORAS является то, что программный продукт, реализующий эту методику, распространяется бесплатно и не требует значительных ресурсов для установки и применения.

- ***Оценка MSAT (качественный подход)***

Ключевыми показателями для данного программного продукта являются: профиль риска для бизнеса и индекс эшелонированной защиты (сводная величина уровня защищенности).

MSAT позволяет оценить эффективность инвестиций, вложенных во внедрение мер безопасности, но не дает возможности найти оптимальный баланс между мерами, направленными на предотвращение, выявление, исправление или восстановление информационных активов.

Как видно, каждый из программных продуктов имеет свои достоинства и недостатки. Отметим, что для наиболее полного анализа рисков не только на техническом, но и на организационном уровне, наиболее подходящими являются MSAT, RiskWatch и ГРИФ. Однако качественно-количественный подход применяется только в RiskWatch и ГРИФ. Для разовой оценки рисков подойдет бесплатный вариант CORAS. Для управления рисками на базе периодических оценок на техническом уровне лучше всего подходит CRAMM.

Заключение

В докладе был рассмотрен и проанализирован процесс анализа и оценки рисков. Была подчеркнута необходимость и важность использования системы оценки и анализа рисков при проектировании системы обеспечения информационной безопасности. Показано, что игнорирование данного подхода может привести к неоправданно высоким затратам на построение системы ИБ. Приведена модель Клементса-Хоффмана, в процессе анализа которой и была поднята проблема управления рисками.

Также описаны и проанализированы основные методики управления рисками. Был сделан вывод о том, что наиболее эффективно использовать подход, сочетающий в себе как качественную, так и количественную оценку рисков.

Проведен анализ нескольких существующих программных продуктов для управления рисками. Каждый из продуктов имеет свои достоинства и недостатки, но сфера их применения

зависит от самого предприятия. В некоторых случаях минусы данного продукта не являются важными для конкретной компании.

Литература

1. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408: 2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
2. Международный стандарт ISO/IEC 27005:2008. Информационная технология – Методы защиты – Менеджмент рисков информационной безопасности.
3. Хоффман Л.Дж. Современные методы защиты информации // Пер. с англ. – М.: Советское радио, 1980. – 264 с.
4. Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р. Оптимизация выбора состава средств инженерно-технической защиты информации на основе модели Клементса-Хофмана // Вестник Брянского ГТУ, 2008. – № 1. – С. 61-67.
5. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 31010:2009. Менеджмент риска. Методы оценки риска.
6. Баранова С.Ю. Методики анализа и оценки рисков информационной безопасности, Вестник Московского университета им. С.Ю. Витте. Серия 3. Образовательные ресурсы и технологии, 2015. – № 1(9). – С. 73-79.
7. Разумников С.В. Анализ возможности применения методов OCTAVE, RiskWatch, CRAMM для оценки рисков ИТ для облачных сервисов // Современные проблемы науки и образования, 2014. – № 1. – С. 247-248.
8. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность // Петренко С.А., Симонов С.В. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.
9. Максименко В.Н., Даричева А.Н. Методические подходы к оценке качества услуг контакт-центра // Экономика и качество систем связи, 2017. – № 1(3). – С. 79-88.
10. Максименко В.Н., Ясюк Е.В. Сравнительный анализ методических подходов к оценке рисков информационной безопасности // в сборнике: Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом. 2017. – С. 15-16.