*2001 р. – Вип. 2. – С. 31–39. 3. Господарський процесуальний кодекс України № 1798-XII від 6 листопада 1991 року // Відомості Верховної Ради (ВВР) 1992, № 6, ст. 56 із змінами станом на 21. 06. 2001 р. (Закон України № 2539-III від 21. 06. 2001, ВВР, 2001, № 36, ст. 188). 4. Закон України "Про судоустрій" № 3018-III від 7 лютого 2002 року // Урядовий Кур'єр № 58, 27 березня 2002 р. Орієнтир. – № 12, 2002 р. 5. Михеєнко М. М., Нор В. Т., Шибіко В. П. Кримінальний процес України: Підручник. – 2-ге вид., перероб. і доп. – К.: Либідь, 1999. – С. 47. 6. Конституція України // Відомості Верховної Ради (ВВР), 1996, № 30, ст. 141. 7. Закон України "Про статус суддів" № 2862-XII від 15 грудня 1992 року // Відомості Верховної Ради (ВВР), 1993, № 8, ст. 56 із змінами станом на 21. 06. 2001 р. (Закон України № 2539-III від 21. 06. 2001, ВВР, 2001, № 36, ст. 188). 8. Закон України "Про державну службу" № 3723-XII від 16 грудня 1993 року // Відомості Верховної Ради (ВВР), 1993, № 52, ст. 490 зі змінами і доповненнями.*

**УДК 381.322**

# СОВРЕМЕННОЕ СОСТОЯНИЕ МЕТОДОЛОГИИ АНАЛИЗА РИСКОВ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СИСТЕМЫ

***Елена Высоцкая, Анатолий Давиденко***
*Национальный авиационный университет*

*Аннотация:* **Рассматривается современное состояние методологии анализа рисков при обеспечении информационной безопасности компьютерных систем. Рассматриваются цели анализа рисков, его этапы, подходы к проведению анализа, а также существующие программные продукты, с помощью которых можно проанализировать риски. Определяются основные тенденции развития методов анализа рисков.**

*Summary:* **This article deals with the contemporary state of risk analysis methodology while supporting the information security of computer systems. The purposes of risk analysis, its stages, approaches to the execution of analysis, as well as the existent program products by means of which the risks can be analyzed are being considered here. The basic tendencies of the development of risk analysis methods are determined.**

*Ключевые слова:* **Информационная безопасность, анализ рисков, защита информации, системы защиты информации.**

Сейчас все больше организаций используют в своей работе информационные системы. С одной стороны это облегчает их работу и повышает ее эффективность, а с другой – порождает новую проблему – необходимость обеспечения защищенности информационной системы. При обеспечении информационной безопасности важно использовать комплексный подход, сочетающий меры на разных уровнях:

- на административном уровне (политика безопасности организации);
- на процедурном уровне (меры безопасности, реализуемые персоналом);
- на программно-техническом уровне (конкретные технические меры: резервное копирование, антивирусная и парольная защита, межсетевые экраны, шифрование данных и т. д.).

В некоторых организациях достаточно обеспечить базовый уровень информационной безопасности, а в некоторых к безопасности информации предъявляются повышенные требования. Однако, и в том, и в другом случае основным этапом является анализ рисков (здесь и далее по тексту подразумевается – анализ рисков при защите информации в информационных системах). Поэтому рассмотрим этот этап подробнее.

Существуют различные методики анализа рисков. Некоторые основаны на качественных оценках рисков, другие – на количественных. Однако при рассмотрении этих методик применительно к конкретной информационной системе возникают проблемы. Кроме того, при постоянном росте информационных технологий большинство методик и программных продуктов на их основе оказываются устаревшими. Поэтому можно сказать, что технология анализа риска сегодня развита слабо.

Какие же цели у анализа риска, в чем он заключается, и какие методики анализа риска сегодня существуют?

Целью анализа риска является оценка угроз и уязвимостей, определение комплекса контрмер, обеспечивающего достаточный уровень защищенности информационной системы. Также целью процесса оценивания рисков является определение характеристик рисков информационной системе и ее ресурсам. На основе таких данных могут быть выбраны необходимые средства защиты.

Существуют различные подходы к оценке рисков, выбор которых зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности (ИБ).

В общем случае процесс оценивания рисков содержит несколько этапов:

- описание объекта и мер защиты;
- идентификация ресурса и оценивание его количественных показателей (определение потенциального негативного воздействия на бизнес);
- анализ угроз информационной безопасности;
- оценивание уязвимостей;
- оценивание существующих и предполагаемых средств обеспечения информационной безопасности;
- оценивание рисков.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация, и зависит от:

- показателей ценности ресурсов;
- оценки значимости угроз;
- оценки значимости уязвимостей;
- вероятностей нанесения ущерба ресурсам (выражаемых через вероятности реализации угроз для ресурсов);
- степени легкости, с которой уязвимости могут быть использованы при возникновении угроз (уязвимости системы защиты);
- от эффективности существующих или планируемых средств обеспечения ИБ.

Расчет этих показателей выполняется на основе математических методов, имеющих такие характеристики, как обоснование и параметры точности метода.

Информационная система в зависимости от своего класса должна обладать подсистемой безопасности с определенными формальными свойствами.

В зависимости от оценки собственниками ценности своих информационных ресурсов и возможных последствий нарушения режима информационной безопасности используются два подхода к анализу рисков:

- базовый анализ рисков;
- полный анализ рисков.

При базовом анализе рисков предполагается, что ценность защищаемых ресурсов, с точки зрения организации, не является чрезмерно высокой (не оценивается) и анализ рисков производится по упрощенной схеме: рассматривается стандартный набор наиболее распространенных угроз безопасности (вирусы, сбои оборудования, несанкционированный доступ и т. д.) без оценки их вероятности. В этом случае обеспечивается минимальный или базовый уровень ИБ (т. е. характеристики угроз при этом рассматривать не обязательно).

При проведении полного анализа рисков необходимо:

- определить ценность ресурсов;
- к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;
- оценить вероятность угроз;
- определить уязвимость ресурсов;
- предложить решение, обеспечивающее необходимый уровень ИБ.

Сначала необходимо разделить все защищаемые ресурсы на классы.

Ресурсы обычно подразделяются на несколько классов, например:

- физические;
- программные;
- данные.

Для каждого класса должна существовать своя методика оценивания ценности элементов, помогающая выбрать подходящий набор критериев. Эти критерии используются для описания потенциального ущерба, связанного с нарушением конфиденциальности и целостности информационной системы, а также уровня ее доступности.

Физические ресурсы оцениваются с точки зрения стоимости их замены или восстановления работоспособности. Эти стоимостные величины затем преобразуются в ранговую (качественную) шкалу, которая используется также для информационных ресурсов.

Программные ресурсы оцениваются тем же способом, что и физические, на основе определения затрат на их приобретение или восстановление.

Если для информационного ресурса существуют особенные требования к конфиденциальности или целостности, то оценка этого ресурса производится по той же схеме, т. е. в стоимостном выражении.

В зависимости от профиля организации, в которой используется данная информационная система, могут использоваться и другие критерии.

Ресурсы должны быть проанализированы с точки зрения оценки воздействия возможных атак (спланированных действий внутренних или внешних злоумышленников) и различных нежелательных событий естественного происхождения. Такие потенциально возможные события называются угрозами безопасности. Уязвимости – это слабые места в системе защиты, которые делают возможной реализацию угроз.

Вероятность того, что угроза реализуется, определяется следующими основными факторами:

- привлекательностью ресурса (этот показатель учитывается при рассмотрении угрозы умышленного воздействия со стороны человека);
- возможностью использования ресурса для получения дохода (показатель учитывается при рассмотрении угрозы умышленного воздействия со стороны человека);
- простотой использования уязвимости при проведении атаки.

Сегодня существуют различные подходы к анализу риска. Но одним из наиболее важных соображений при выборе методологии или техники анализа риска является то, что результаты, полученные из оценки риска, должны быть полезны при обеспечении защиты информационной системы. Если методология очень сложна при ее использовании, если она требует очень точных исходных данных, или если ее результаты слишком сложны для того, чтобы сделать вывод, каким является реальный риск, то эта методология не будет полезна и не поможет создать эффективную защиту системы. С другой стороны, если методология не позволяет добиться приемлемой точности при определении значений таких переменных, как потери, вероятности и стоимости, полученные результаты могут оказаться слишком простыми и не отражать истинного риска. Необходимо использовать такой подход для оценки риска, который бы обеспечивал применение методики, являющейся понятной, легко используемой, и приводящей к результатам, которые помогают организации эффективно защищать свои ресурсы.

В 1979 Национальный институт стандартов и технологии США (NIST – National Institute of Standards and Technology) издал Федеральный стандарт по обработке информации (FIPS 65 – Federal Information Processing Standard), который описал количественный метод для выполнения анализа риска. Этот документ был выпущен как рекомендация, а не как стандарт. Поэтому использование FIPS 65 не является обязательным при выполнении анализа риска. Этот метод в основном предназначался для проведения анализа риска в больших центрах обработки данных. Данный стандарт описывает, как можно получить оценку риска (то есть ожидаемые ежегодные потери) для каждого файла данных приложений, оценив частоту возникновения вредного воздействия (то есть разрушения, модификации, раскрытия или недоступности файла данных) и последствия (в долларах), которые могут возникнуть в результате каждого из воздействий. Признавая отсутствие эмпирических данных относительно частоты возникновения воздействий и связанных с ними последствий, FIPS 65 предложил использовать подход с применением порядка величины для аппроксимации этих значений. Из-за того, что эта концепция была не понята людьми, использовавшими это метод, было много попыток получить слишком точные значения для исходных данных FIPS 65 и, как следствие, интерпретировать результаты как имеющие большую точность, чем есть на самом деле.

Имеется ряд автоматизированных средств анализа риска, которые были специально разработаны для анализа среды. Существует большое количество преимуществ от использования автоматизированных средств анализа риска. Однако возникает ряд проблем при использовании автоматизированных инструментов анализа риска. Имеется большое количество методов для вычисления риска. В то время как большинство из этих методов зависят от значений потерь и значений вероятностей, представление значений этих переменных, вычисления, производимые с этими переменными, и способ интерпретации значения риска не всегда доступны пользователю. Этот недостаток усиливается из-за того, что в настоящее время не имеется стандартного метода или согласованного подхода для выполнения анализа риска. В то время как для анализа риска существует вариант стандартной схемы его проведения, который дает разработчикам программ некоторые рекомендации по разработке этих инструментов, нет согласия в отношении методов представления переменных, необходимых для выполнения анализа риска, и в отношении методов для вычисления риска на основе этих переменных. Из-за отсутствия согласия среди специалистов по анализу риска, вкупе со специфичностью данных инструментов, определение эффективности конкретного метода может быть проблематичным. С другой стороны, если методология, используемая средством, понятна и считается пользователем приемлемой, то средство может оказаться вполне адекватным. Основной вопрос при определении того, будет ли инструмент эффективен для специфической окружающей среды, должен звучать так: "Что измеряет данное средство анализа риска, и полезны ли для обеспечения требуемой защиты данной информационной системы результаты, полученные при помощи этого средства?"

Другой подход при выполнении анализа риска состоит в разработке базовых наборов средств и мер защиты, необходимых для заранее определенных стандартных уровней риска. Стандартные уровни риска могут быть основаны на ценности ресурсов как таковых (например, данные считаются критичными из-за политики организации или федерального закона), на последствиях, которые могут последовать после потери ценности (например, организация не сможет выполнить задачу) или на других факторах. Это позволяет владельцам данных и ответственным за обеспечение безопасности системы определять уровень риска для определенных ценностей, следовать рекомендациям в отношении полученного уровня риска и внедрять меры защиты, которые считаются адекватными. Этот подход может быть полезен для организации благодаря реализации согласованной защиты для конкретных типов ценностей. Этот подход был неоднократно реализован. Выгода от этого подхода заключается в том, что пользователя не только обеспечивают методологией анализа риска, но также информацией, позволяющей понимать политику безопасности организации, основанную на базовых наборах средств и мер защиты.

Существуют и другие методологии и подходы. Некоторые требуют ручной обработки; другие реализованы программно. Некоторые методики основаны на достаточно простых табличных методах и не предполагают применения специализированного ПО, другие, наоборот, его используют.

В табличных методах можно наглядно отразить связь факторов негативного воздействия (показателей ресурсов) и вероятностей реализации угрозы с учетом показателей уязвимостей. Эти методы состоят из нескольких шагов.

Рассмотрим для примера один из таких методов.

На первом шаге оценивается негативное воздействие (показатель ресурса) по заранее определенной шкале (скажем, от 1 до 5) для каждого ресурса, которому угрожает опасность.

На втором – по той же шкале оценивается вероятность реализации каждой угрозы.

На третьем шаге вычисляется показатель риска. В простейшем варианте методики это делается путем умножения показателя негативного воздействия на вероятность реализации каждой угрозы. Но операция умножения определена для количественных шкал. Для ранговых (качественных) параметров, каковыми являются показатель негативного воздействия и вероятность реализации угрозы, показатель риска не всегда вычисляется математическим умножением (2*5 не всегда равно 5*2). Соответственно, применительно к конкретной организации должна быть разработана методика оценки показателей рисков.

На четвертом шаге угрозы ранжируются по значениям их фактора риска.

Применение каких-либо инструментальных средств не является обязательным, однако, позволяет уменьшить трудоемкость анализа рисков и выбора контрмер. В настоящее время есть много программных продуктов для анализа рисков: от простейших, ориентированных на базовый уровень безопасности, до сложных и дорогостоящих, позволяющих реализовать полный вариант анализа рисков и выбрать комплекс контрмер требуемой эффективности.

Для того чтобы обеспечить базовый уровень безопасности, достаточно проверить выполнение требований соответствующего стандарта (спецификации). Программные продукты, предназначенные для этой цели, позволяют сформировать список вопросов, касающихся выполнения этих требований. На основе ответов генерируется отчет с рекомендациями по устранению выявленных недостатков.

Примером программного продукта этого класса является COBRA, производитель C&A Systems Security Ltd. COBRA позволяет существенно облегчить процесс проверки на соответствия требованиям Британского стандарта BS 7799 (ISO 17799) информационной системы. Есть несколько баз знаний: общие требования BS 7799 (ISO 17799) и специализированные базы, ориентированные на различные области применения. COBRA позволяет представить требования стандарта в виде тематических "вопросников" по отдельным аспектам деятельности организации.

Еще один пример – RiskPAC, производитель CSCI. Этот программный продукт позволяет проверить на соответствие требованиям базового уровня защищенности организации CSCI. Возможна настройка на различные области применения путем добавления или исключения дополнительных вопросов. Кроме того, есть калькулятор ожидаемых среднегодовых потерь, позволяющих оценить ожидаемые потери по различным видам информационных ресурсов.

В обоих программных продуктах имеются средства создания нескольких видов отчетов.

Программные средства, необходимые для полного анализа рисков, строятся с использованием структурных методов системного анализа и проектирования (SSADM – Structured Systems Analysis and Design) и представляют собой инструментарий для выполнения следующих операций:

- построения модели ИС с позиции ИБ;
- оценки ценности ресурсов;
- составления списка угроз и уязвимостей, оценки их характеристик;
- выбора контрмер и анализа их эффективности;

- анализа вариантов построения защиты;
- документирования (генерация отчетов).

Примерами программных продуктов этого класса являются CRAMM (разработчик – компания Logica, Великобритания), MARION (разработчик CLUSIF, Франция), RiskWatch (США). Обязательным элементом этих продуктов является база данных, содержащая информацию по инцидентам в области ИБ, позволяющая оценить риски и уязвимости, эффективность различных вариантов контрмер в определенной ситуации.

Один из возможных подходов к разработке таких методик – это накопление статистических данных о реальных происшествиях, анализ и классификация их причин, выявление факторов риска. На основе этой информации можно оценить угрозы и уязвимости в других информационных системах. Но при реализации этого подхода возникают практические сложности. Во-первых, должен быть собран весьма обширный материал о происшествиях в этой области. Во-вторых, применение этого подхода оправданно далеко не всегда. Если информационная система достаточно крупная (содержит много элементов, расположена на обширной территории), имеет давнюю историю, то подобный подход, скорее всего, применим. Если система сравнительно невелика, использует только новейшие элементы технологии (для которых пока нет достаточной статистики), оценки рисков и уязвимостей могут оказаться недостоверными.

Альтернативой статистическому подходу является подход, основанный на анализе особенностей технологии. Но он также не универсален, т. к. темпы технологического прогресса в области информационных технологий таковы, что имеющиеся оценки относятся к уже устаревшим или устаревающим технологиям, для новейших технологий таких оценок или вообще нет, или их очень мало.

Одним из наиболее известных продуктов этого класса является CRAMM.

В 1985 г. был разработан метод, соответствующий требованиям ССТА (Центральное агентство по компьютерам и телекоммуникациям Великобритании). Он получил название CRAMM – метод ССТА анализа и контроля рисков. Затем появилось несколько его версий, ориентированных на требования министерства обороны, гражданских государственных учреждений, финансовых структур, частных организаций. Одна из версий, “коммерческий профиль”, является коммерческим продуктом. В настоящее время продается версия CRAMM 4.0.

Целью разработки метода являлось создание формализованной процедуры, позволяющей:

- убедиться, что требования, связанные с безопасностью, полностью проанализированы и документированы;
- избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков;
- оказывать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем;
- обеспечить проведение работ в сжатые сроки;
- автоматизировать процесс анализа требований безопасности;
- представить обоснование для мер противодействия;
- оценивать эффективность контрмер, сравнивать различные варианты контрмер;
- генерировать отчеты.

Анализ рисков включает в себя идентификацию и вычисление уровней (мер) рисков на основе оценок, присвоенных ресурсам, угрозам и уязвимостям ресурсов.

Контроль рисков состоит в идентификации и выборе контрмер, позволяющих снизить риски до приемлемого уровня.

Формальный метод, основанный на этой концепции, должен позволить убедиться, что защита охватывает всю систему и существует уверенность в том, что:

- все возможные риски идентифицированы;
- уязвимости ресурсов идентифицированы и их уровни оценены;
- угрозы идентифицированы и их уровни оценены;
- контрмеры эффективны;
- расходы, связанные с ИБ, оправданы.

Исследование ИБ системы с помощью CRAMM проводится в три стадии.

На первой стадия анализируется все, что касается идентификации и определения ценности ресурсов системы. В конце этой стадии заказчик исследования будет знать, достаточно ли ему существующей традиционной практики или он нуждается в проведении полного анализа безопасности.

На второй стадия рассматривается все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. В конце данной стадии заказчик получает идентифицированные и оцененные уровни рисков для своей системы.

На третьей стадия происходит поиск адекватных контрмер. По существу это поиск варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика. В конце этой стадии он будет

знать, как следует модифицировать систему в терминах мер уклонения от риска, а также выбора и проработки специальных мер противодействия, ведущих к снижению или минимизации оставшихся рисков.

Каждая стадия объявляется законченной после детального обсуждения и согласования результатов с заказчиком.

Первая стадия – стадия идентификации ресурсов и построения модели информационной системы с точки зрения безопасности – включает следующие шаги:

- определение границ исследования (границ системы);
- идентификации ресурсов (оборудование, данные, программное обеспечение);
- построение модели с точки зрения информационной безопасности;
- определение ценности ресурсов;
- получение отчета и обсуждение отчета с заказчиком.

Определение границ исследуемой системы начинается со сбора следующей информации:

- кто ответственный за физические и программные ресурсы;
- кто является пользователем и как пользователи используют или будут использовать систему;
- какая конфигурация системы.

Вся первичная информация собирается в процессе бесед с менеджерами проектов, менеджером пользователей или другими сотрудниками.

Далее проводится идентификация всех ресурсов, которые находятся внутри границ системы: физических, программных и информационных. Каждый ресурс необходимо отнести к одному из предопределенных классов. После этого строится модель информационной системы с точки зрения информационной безопасности. Для каждого информационного процесса, имеющего самостоятельное значение с точки зрения пользователя и называемого пользовательским сервисом, строится дерево связей используемых ресурсов. Построенная модель позволяет выделить критичные элементы.

Далее, если это вариант полного анализа риска, то необходимо определить ценность ресурсов.

Ценность физических ресурсов в данном методе определяется стоимостью их восстановления в случае разрушения.

Ценность данных и программного обеспечения определяется в следующих ситуациях:

- недоступность ресурса в течение определенного периода времени;
- разрушение ресурса – потеря информации, полученной со времени последнего резервного копирования, или ее полное разрушение;
- нарушение конфиденциальности в случаях несанкционированного доступа штатных сотрудников или посторонних лиц;
- модификация – рассматривается для случаев мелких ошибок персонала (ошибки ввода), программных ошибок, преднамеренных ошибок;
- ошибки, связанные с передачей информации: отказ от доставки, недоставка информации, доставка по неверному адресу.

Для оценки возможного ущерба рекомендуется использовать некоторые из следующих параметров:

- ущерб репутации организации;
- нарушение действующего законодательства;
- ущерб для здоровья персонала;
- ущерб, связанный с разглашением персональных данных отдельных лиц;
- финансовые потери от разглашения информации;
- финансовые потери, связанные с восстановлением ресурсов;
- потери, связанные с невозможностью выполнения обязательств;
- дезорганизация деятельности.

Приведенная совокупность параметров используется в коммерческом варианте метода. В других версиях совокупность может быть иной. Так, в версию, используемую в правительственных учреждениях, добавляются параметры, отражающие национальную безопасность и международные отношения.

Для данных и программного обеспечения выбираются применимые к данной ИС критерии, дается оценка ущерба по шкале со значениями от 1 до 10.

Далее рассматриваются основные сценарии, приводящие к различным негативным последствиям, описываемым в терминах выбранных параметров.

На первой стадии может быть подготовлено несколько типов отчетов (границы системы, модель, определение ценности ресурсов).

Если ценности ресурсов низкие, можно использовать базовый вариант защиты. В этом случае исследователь может пропустить вторую стадию и перейти к третьей стадии. Однако использование второй стадии позволяет построить более эффективную схему защиты.

На второй стадии – стадии анализа угроз и уязвимостей:

- оценивается зависимость пользовательских сервисов от определенных групп ресурсов;
- оценивается существующий уровень угроз и уязвимостей;
- вычисляются уровни рисков;
- анализируются результаты.

Группировка ресурсов производится с точки зрения угроз и уязвимостей.

Оценка уровней угроз и уязвимостей производится на основе исследования косвенных факторов. Программное обеспечение CRAMM для каждой группы ресурсов и каждого из 36 типов угроз генерирует список вопросов, допускающих однозначный ответ.

Уровень угроз оценивается, в зависимости от ответов, как очень высокий, высокий, средний, низкий и очень низкий.

Уровень уязвимости оценивается, в зависимости от ответов, как высокий, средний и низкий.

Возможно проведение коррекции результатов или использование других методов оценки.

На основе этой информации рассчитываются уровни рисков в дискретной шкале с градациями от 1 до 7.

Полученные уровни угроз, уязвимостей и рисков анализируются и согласовываются с заказчиком. Только после этого можно переходить к третьей стадии метода.

На третьей стадии – стадии выбора контрмер – CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. Контрмеры можно объединить в три категории: около 300 рекомендаций общего плана; более 1000 конкретных рекомендаций; около 900 примеров того, как можно организовать защиту в данной ситуации.

На этой стадии можно провести сравнительный анализ эффективности различных вариантов защиты.

Достоинством этого метода является то, что можно достаточно быстро провести анализ риска и у результатов анализа будут достаточно четкое обоснование.

Недостатком этого метода является то, что на некоторых этапах могут использоваться нечеткая и субъективная информация. И, кроме того, этот метод может использоваться только для достаточно стандартных информационных систем, т. к. только для них можно выбрать вариант данного продукта с полностью подходящим перечнем критериев.

Сейчас появилась новая идея нового подхода – теоретико-графового подхода к анализу рисков. Подобный подход позволяет использовать математическую модель в качестве опорного инструмента для доказательства истинности того или иного утверждения, касающегося степени защищенности и инертности исследуемой системы защиты. Однако этот подход пока только теоретический и не имеет практической апробации.

Из всего вышесказанного можно сделать вывод, что ни одна из существующих методик анализа рисков и, тем более, программных продуктов на их основе не являются совершенными. У всех подходов есть свои недостатки, а у некоторых достаточно серьезные. Поэтому актуальным является развитие теории анализа рисков в направлениях:

- разработки математических методов моделирования компьютерных систем с целью анализа рисков;
- практической апробации существующих методов анализа рисков в условиях нечеткого субъективного представления информации о быстро меняющихся технологиях обработки информации;
- разработки программного продукта, оперативно реализующего методики анализа рисков, учитывающих изменяющиеся условия.

**УДК 004.056.5**

# АНАЛИЗ ЗАЩИЩЕННОСТИ МОБИЛЬНЫХ ОПЕРАЦИОННЫХ СИСТЕМ

***Денис Кудин, Владислав Корольков****

*Центр информационной безопасности,*

** Запорожский национальный технический университет*

*Аннотация:* **Анализируются особенности реализации мобильных операционных систем с точки зрения их безопасности. Определяются возможные угрозы, способы внедрения, распространения и исполнения вредоносного кода. Рассматриваются методы формального анализа поведения подсистемы защиты во времени и оценки ее реакции на угрозы вредоносного кода с учетом особенностей упрощенной реализации механизмов защиты в карманных персональных компьютерах.**