УДК 004.089

АНАЛИЗ ПРИМЕНИМОСТИ МЕТОДОВ ОЦЕНКИ РИСКОВ К ПРОЦЕССАМ АУТЕНТИФИКАЦИИ ПРИ УДАЛЕННОМ ЭЛЕКТРОННОМ ВЗАИМОДЕЙСТВИИ

А. Г. Сабанов, заместитель генерального директора ЗАО «Аладдин Р.Д.», доцент кафедры ИУ-10 МГТУ им. Н. Э. Баумана, к.т.н.; asabanov@mail.ru

Представлены методы анализа рисков применительно к процессам аутентификации при удаленном электронном взаимодействии. Рассмотрена применимость наиболее развитых подходов к анализу рисков выполнения основных функций аутентификации. Показано, что более половины известных методов анализа рисков могут быть использованы для оценки рисков аутентификации.

Ключевые слова: *метод, аутентификация, информационная безопасность, анализ рисков, удаленное электронное взаимодействие.*

Введение. При выборе механизмов и средств аутентификации для современных информационных систем, поддерживающих возможность удаленного электронного взаимодействия (УЭВ), необходимо уметь оценивать риски информационной безопасности (ИБ). Под оценкой риска будем понимать процессы идентификации риска, анализа и сравнения полученного значения риска с допустимым уровнем риска для данного предприятия.

Основные методы анализа рисков рассмотрены в [1—7]. Достаточно подробный обзор методов оценки рисков приводится в [8]. Однако при подготовке [8] к печати из рассмотрения выпал стандарт [9], в котором впервые системно изложен 31 метод анализа рисков. В данной работе эти методы анализируются с точки зрения применимости к задачам оценки рисков ИБ для процессов аутентификации в ходе УЭВ. При этом учитываются результаты работ [10—16].

Исходные данные. Для оценки применимости развитых к настоящему времени методов анализа рисков к процессам аутентификации при УЭВ используются результаты работ [10—17], стандарт [9], а также практический опыт исследований, проектирования, построения и сопровождения систем идентификации и аутентификации в десятках крупных и средних организаций различного профиля деятельности, накопленный автором за 12 лет работы в этой сфере.

Рекомендации стандартов. Согласно стандартам [1—7, 9], для анализа рисков сначала следует подробно описать область определения. С этой целью в [12] рассмотрены основные процессы аутентификации (ПА), в [13] разработана классификация ПА, а в [14] проведен анализ и представлена классификация систем идентификации и аутентификации (СИА) по признакам соответствия требованиям ИБ. В дополнение к проведенным исследованиям выполнен анализ нормативной базы по ПА, в котором подробно рассмотрены технологии и средства аутентификации [15], а также особенности их функционирования.

На втором этапе анализа рисков стандартами [1—7, 9] рекомендуется провести работы по идентификации рисков. Здесь должны быть определены опасные события, частота и вероятность их наступления. Для СИА результаты таких исследований представлены в [11], причем следует отметить такой интересный результат, как вывод о необходимости введения уровней достоверности аутентификации (УДА), вытекающий из анализа угроз и уязвимостей процедур регистрации нового пользователя ИС. Также обоснованием введения УДА служит анализ процедур хранения и предъявления аутентификационной информации пользователя.

Следующий этап оценки рисков, как рекомендуется в [1—7, 9], представляет собой непосредственно процедуру анализа рисков. Для рисков аутентификации наиболее приемлемым способом является многоуровневый анализ рисков [16]. Суть многоуровневого анализа на основе процессного подхода состоит в рассмотрении СИА на разных уровнях детализации. На первом уровне СИА исследуется как отдельный, но при этом целый элемент ИС, на втором уровне анализируются процедуры, составляющие процесс аутентификации в СИА, на третьем — риски выполнения функций отдельных элементов СИА, например серверная или клиентская часть, канал связи клиент-сервер и т.д. При необходимости можно опуститься и на следующий уровень детализации, такой как уровень ключевого носителя, в котором хранится аутентификатор. Принципы моделирования и наглядные примеры изложены в [17].

Результаты оценивания рисков аутентификации могут использоваться, с одной стороны, в качестве исходных данных для итеративного процесса анализа рисков и их снижения до приемлемого уровня, а с другой — итоговые значения рисков (после итераций) можно применять для уточнения границ достоверности аутентификации. Попробуем оценить применимость наиболее известных методов анализа рисков — это может оказаться полезным для понимания возможных способов снижения рисков при построении и эксплуатации СИА, а также при выборе средств аутентификации.

Краткое описание методов анализа рисков. Представим рассматриваемые методы в общем виде, акцентируя внимание на применимости входных и выходных данных для решения задачи оценки рисков аутентификации при УЭВ. Полное описание методов и особенностей их применения можно найти в источниках, приведенных в списке литературы.

1. *Метод «мозгового штурма»* представляет собой обсуждение проблемы группой специалистов с целью идентификации возможных видов отказов и соответствующих опасностей, риска, критериев принятия решений и/или способов обработки риска. Входные данные: команда специалистов, обладающих знанием организации, системы, процессов, которые необходимо оценить. Выходные данные: идентифика-

ция рисков, перечни опасных событий и средства противодействия угрозам.

2. *В структурированном интервью* опрашиваемому задают вопросы из заранее подготовленного перечня, позволяющие провести всесторонний анализ ситуации и получить более полную идентификацию опасностей и риска. Входные данные: точное определение целей интервью, продуманный список опрашиваемых экспертов, перечень вопросов. Выходные данные: информация о восприятии экспертами проблем, которые являются предметом интервью.

3. *Метод Дельфи* [18] предназначен для получения обобщенного мнения группы экспертов. Особенностью метода является то, что эксперты выражают свое мнение индивидуально и анонимно, при этом имея возможность узнать мнения своих коллег. Входные данные: варианты решений, для отбора которых необходимо согласованное единое мнение. Выходные данные: единое мнение экспертов по проблеме.

4. *Предварительный анализ опасностей* (Preliminary Hazard Analysis, PHA) является простым индуктивным методом анализа с целью идентификации опасностей, критических ситуаций и событий, которые могут нарушить работу СИА или нанести ей вред. Пример проведения анализа по идентификации рисков с помощью PHA приводится в [10]. Входные данные: детализированная информация об оцениваемой системе. Выходные данные: перечень опасностей и соответствующего риска, а также рекомендации по управлению и/или принятию риска.

5. *Исследование опасности и работоспособности* (Hazard and Operability Study, HAZOP) — это метод идентификации опасностей и риска выполнения функций аутентификации для СИА. HAZOP (МЭК 61882) является качественным методом анализа рисков: он формирует конкретные предложения по обработке риска. Исследование HAZOP направлено на идентификацию видов отказов процесса, системы или процедур, их причин и последствий. Отличие HAZOP от метода FMEA (см. п. 7) заключается в том, что при применении исследования HAZOP рассматривают нежелательные результаты и отклонения от намеченных результатов и условий для поиска возможных причин и видов отказа, тогда как в методе FMEA анализ начинают с идентификации видов отказа. Входные данные: текущая информация об исследуемой СИА, составляющих ее функционал процессах и процедурах, а также о целях и функциональных требованиях к проекту. Выходные данные: систематическое и полное исследование системы, процесса или процедуры экспертами, содержащее возможные причины, предложенные действия по идентифицированным рискам и назначение ответственного за эти действия.

6. *Анализ воздействий* (Business Impact Analysis, BIA) позволяет понять, как ключевые виды отказов/нарушений/разрушений могут повлиять на ключевые процессы СИА, а также идентифицировать и количественно определить необходимые возможности для управления СИА в этих условиях. Входные данные для экспертов, специализирующихся на вопросах непрерывности бизнеса: информация о целях, окружающей среде, составе и функционале СИА, ресурсах, соглашения об аутсорсинге, подрядчиках, экономических и производственных последствиях, вызванных нарушением критических процессов. Выходные данные: перечень ранжированных по приоритетам критических процессов и соответствующих взаимозависимостей, оценки ресурсов на восстановление, возможные сроки простоя (Maximum Acceptable Outage, MAO) и восстановления критических процессов и взаимосвязанных информационных технологий.

7. *Анализ видов и последствий отказов* (Failure Mode Effect Analysis, FMEA; МЭК 60812, ГОСТ Р 51901.12—2007) применяется для идентификации способов отказа компонентов, систем или процессов СИА, которые могут привести к невыполнению ее функционала. Является методом количественного анализа. Метод применим к видам отказов, связанных с ошибками персонала, нарушением работоспособности оборудования и систем программного обеспечения и процессов. Пример использования FMEA к анализу СИА приведен в [11]. Входные данные: подробная информация об элементах системы, достаточная для анализа способов и путей развития отказа каждого элемента. Выходные данные: перечень видов отказа, механизмов возникновения отказа и его последствий для каждого компонента системы и этапа процесса, результаты ранжирования значимости отказов на основе оценки вероятности отказа системы, уровня риска возникновения данного вида отказа. Существенными недостатками метода являются применимость для идентификации только отдельных отказов, а не их сочетания, а также трудоемкость и длительность для сложных многоуровневых систем класса развитой СИА.

8. *Анализ дерева неисправностей* (Fault Tree Analysis, FTA; МЭК 61025) — более сложный и ориентированный на получение характеристик надежности метод, который используется для определения качественной оценки при идентификации причин отказа и путей, приводящих к конечному событию, и количественной оценки при вычислении вероятности конечного события, если известны значения вероятностей начальных событий. Пример применения FTA к СИА приводится в [19]. Входные данные: хорошее знание системы и понимание причин отказа, а также знание того, как система может выйти из строя. Для анализа полезно использование детальных схем дерева неисправностей. Выходные данные: наглядное представление путей возникновения конечного события в ситуации, когда одновременно могут произойти два события или более; набор минимальных сечений (возникновения путей отказа системы) и оценка вероятности отказа системы для каждого сечения; оценка вероятности конечного события.

9. *Анализ дерева событий* (Event Tree Analysis, ETA) является графическим методом представления взаимоисключающих последовательностей событий, возникающих после появления исходного события, в соответствии с функционированием СИА. Пример анализа приводится в [19]. Входные данные: перечень рассматриваемых начальных событий, информация о способах обработки, средствах управления и соответствующих вероятностях отказа (для количественного анализа). Выходные данные: качественное описание возможных проблем в виде комбинаций событий, представляющих собой различные следствия начального события (ранжирование последствий); количественные оценки частоты или вероятности появления событий и относительной значимости различных последствий отказа и способствующих им событий; перечень рекомендаций по снижению риска и количественные оценки эффективности внедрения рекомендаций. В целом применение данного метода является трудоемкой задачей и может оцениваться как анализ высокого уровня сложности.

10. *Попарный анализ «причина — последствие»* сочетает в себе методы дерева неисправностей и дерева событий. Диаграммы сложны в построении и применении, поэтому их целесообразно использовать, когда потери от последствий отказов сопоставимы с затраченными усилиями. Входная инфор-

мация: знание системы, видов и сценариев отказов. Выходные данные: схематическое представление отказа системы с указанием причин и последствий и оценка вероятности возникновения каждого потенциального последствия, основанная на анализе вероятностей возникновения соответствующих условий после критического события.

11. *Анализ уровней защиты* (Layers of Protection Analysis, LOPA) — смешанный метод оценки риска, связанного с нежелательным событием или сценарием. Метод направлен на анализ достаточности мер по управлению или снижению риска. Основан на выборе пар причин и последствий и идентификации уровней защиты, способных предотвратить событие, которое может стать причиной нежелательного последствия. Для определения адекватности мер снижения риска до допустимого уровня необходимо провести расчет последствий. Входные данные: основная информация о риске, включая опасности, причины и последствия; частота событий причины отказа, оценки вероятности отказа уровней защиты, оценки последствий и допустимого риска. Выходные данные: рекомендации по применению средств управления риском и их эффективности защиты для снижения риска.

12. *Анализ дерева решений* позволяет последовательно представить альтернативные варианты решений с их выходными данными и соответствующей неопределенностью. Используется на стадии проектирования. Как и при выполнении анализа дерева событий, построение следует начинать с исходного события или с принятого решения. Входные данные: план проекта СИА с указанием пунктов, по которым необходимо принять решение, информация о возможных результатах принятых решений и события, влияющие на эти решения. Выходные данные: логический анализ риска, отражающий различные варианты возможных решений, и ожидаемое значение риска для каждого возможного пути решения.

13. *Анализ влияния человеческого фактора* (Human Reliability Assessment, HRA) применяют для оценки влияния действий человека на работу системы. Входные данные: информация о задачах, выполняемых человеком, данные о типичных ошибках, встречающихся на практике, и их причинах. Выходные данные: качественная или количественная оценка риска рассмотренных ошибок, которые могут произойти, и методы их снижения.

14. *Анализ «галстук-бабочка»* представляет собой схематический способ описания и анализа пути развития опасного события от причин до последствий. Данный метод сочетает исследование причин события с помощью дерева неисправностей и анализ последствий с помощью дерева событий [20]. Входные данные: информация о причинах и последствиях опасных событий, риске, СЗИ, а также о средствах управления, которые могут их предотвратить или смягчить. Выходные данные: простая диаграмма, показывающая основные пути опасных событий и установленные барьеры, направленные на предотвращение или смягчение нежелательных последствий.

15. *Марковский анализ* (МЭК 61078, ГОСТ Р 51901.15—2006) применим в ситуации, когда будущее состояние системы зависит только от ее текущего состояния. Полумарковские методы (метод вложенных цепей Маркова) также могут использоваться для анализа СИА [16]. Входные данные: перечень различных состояний системы, подсистемы или компонента (например, полное функционирование, частичное функционирование, ухудшение состояния), отказ системы и понимание возможных переходов ее из одного состояния в другое. Выходные данные: вероятности пребывания системы в различных состояниях, а следовательно, и оценки вероятностей отказа и/или безотказной работы компонентов системы.

16. *Матрица последствий и вероятностей* служит средством объединения качественных или смешанных (количественных и качественных) оценок последствий и вероятностей; метод применяется для определения или ранжирования уровня риска. Входные данные: шкалы последствий и вероятностей, установленные в соответствии с запросами потребителя, и матрица, которая их объединяет. Уровни риска, принятые для ячеек таблицы, зависят от определений, применяемых для шкал вероятности и последствий. Выходные данные: класс каждого опасного события или перечень опасных событий с указанием уровня значимости последствий и вероятности их наступления.

17. *Анализ эффективности затрат* используют для оценки риска в ситуации, когда необходимо сравнить общие ожидаемые затраты с общими ожидаемыми выгодами (доходами и преимуществами) и выбрать лучший или наиболее выгодный вариант. Входные данные: информация о затратах и выгодах и об оценке неопределенности этих затрат и выгод. Выходные данные: информация об относительных затратах и выгодах при различных вариантах решений или действий.

18. *Мультикритериальный анализ* (Multiple criteria decision Analysis, MCDA) предполагает ранжирование критериев для объективной и прозрачной оценки различных вариантов решений. В конечном итоге необходимо определить и расставить по предпочтениям доступные варианты решений. Анализ включает в себя разработку матрицы вариантов и критериев, которые следует ранжировать и объединить для выполнения общей оценки каждого варианта решения. Входные данные: набор вариантов решений для проведения анализа. Выходные данные: результаты ранжирования вариантов по убыванию предпочтений.

Заметим, что на практике применяется сразу несколько методов в различных комбинациях.

После рассмотрения непосредственно самих методов можно приступить к анализу их применимости к оценке рисков СИА.

Критерии применимости методов анализа рисков. Оценка производилась методом Дельфи [18]. При рассмотрении вопроса о применимости методов анализа рисков для оценки и управления рисками аутентификации при УЭВ выбраны следующие критерии:

- оценка объема подготовительных работ для последующего анализа данным методом;
- доступность исходных (входных) данных;
- оценка применимости выходных данных для последующего анализа;
- наглядность результатов;
- удобство анализа с применением данного метода.

Выбор критериев обусловлен опытом практического применения методов анализа рисков к процессам аутентификации при УЭВ.

Оценка применимости. Для проведения оценки методов анализа рисков был произведен предварительный отбор методов по их назначению. Априори ненужные для анализа ИБ-рисков методы (например, метод оценки токсикологического риска и др.) были сразу исключены из рассмотрения. Также из списка методов изъяты те, которые в стандарте [9] не рекомендованы к применению для процессов идентификации риска и анализа риска (например, метод Монте-Карло, байесовский анализ и др.). В итоге из представленных в [9] методов оценки

Оценка применимости методов анализа рисков для аутентификации при УЭВ

	Метод	Объем подготовительных работ	Доступность входных данных	Применимость выходных данных	Наглядность результатов	Удобство анализа
1	Мозговой штурм	Н	Н	С	С	С
2	Структурированное интервью	Н	С	Н	С	Н
3	Метод Дельфи	Н	Н	С	С	С
4	Предварительный анализ опасностей (PHA)	Н	С	В	В	В
5	Исследование опасности и работоспособности (HAZOP)	С	С	С	С	С
6	Анализ воздействий (BIA)	С	С	С	С	С
7	Анализ видов и последствий отказов (FMEA)	С	Н	В	С	В
8	Анализ дерева неисправностей (FTA)	Н	С	С	В	В
9	Анализ дерева событий (ETA)	В	В	В	В	В
10	Попарный анализ «причина-последствие»	С	С	В	В	В
11	Анализ уровней защиты (LOPA)	С	С	В	С	С
12	Анализ дерева решений	В	С	С	В	С
13	Анализ влияния человеческого фактора (HRA)	С	В	С	С	С
14	Анализ «галстук-бабочка»	В	В	С	С	С
15	Марковский анализ	В	В	С	В	В
16	Матрица последствий и вероятностей	С	В	В	В	В
17	Анализ эффективности затрат (CBA)	В	С	С	В	В
18	Мультикритериальный анализ решений (MCDA)	В	С	В	В	В

риска аутентификации в таблицу вошли только 18.

Для удобства восприятия в таблице использованы следующие принятые в международных и отечественных стандартах обозначения уровней: Н — низкий, С — средний, В — высокий.

Как следует из таблицы, для анализа рисков аутентификации при УЭВ имеется достаточно широкий набор приемлемых методов. Выбор методов оценки рисков зависит от конкретных обстоятельств: масштаба и состава информационной системы, информации, обрабатываемой данной ИС, состава и используемых средств аутентификации, наличия квалифицированных экспертов и т.д.

Заключение. Результаты статьи могут быть использованы в практике анализа рисков аутентификации. Проведенное исследование имеет свои плюсы и минусы. Главным минусом работы, основанной на исследованиях автора, является ее субъективный характер. Достоинством можно назвать ориентированность на практические результаты.

В развитие работы планируется провести исследование применимости наиболее широко используемых методов управления рисками для анализа рисков аутентификации. В перспективе будут рассмотрены особенности методов оценки надежности и качества аутентификации при УЭВ. Конечной целью планируемого исследования должна стать разработка рекомендаций для внесения изменений в нормативную базу регулирования процессов идентификации и аутентификации, а также рекомендаций по учету требований безопасности и надежности при проектировании и построении систем идентификации и аутентификации в государственных информационных системах.

ЛИТЕРАТУРА

1. ГОСТ Р 51897—2011. Менеджмент риска. Термины и определения.
2. ГОСТ Р 51901.1—2002 (все части). Менеджмент риска. Анализ риска технологических систем.
3. ГОСТ Р ИСО/МЭК 13335—1—2006 (все части). Информационная технология. Методы и средства обеспечения безопасности.
4. ГОСТ Р ИСО/МЭК 27001—2006. Информационная технология. Методы обеспечения информационной безопасности. Системы менеджмента информационной безопасности. Требования.
5. ГОСТ Р ИСО/МЭК 16085—2007. Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения.
6. ГОСТ Р ИСО/МЭК 27005—2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
7. ГОСТ Р ИСО 31000—2010. Менеджмент риска. Принципы и руководство.
8. **Сабанов А.Г.** Об оценке рисков удаленной аутентификации //Электросвязь.— 2013.— № 4.
9. ГОСТ Р ИСО 31010—2011. Менеджмент риска. Методы оценки риска.
10. **Сабанов А.Г**. Методика идентификации рисков аутентификации //Докл. Томского гос. ун-та систем управления и радиоэлектроники.— 2013.— № 4 (30).
11. **Сабанов А.Г**. Многоуровневый анализ угроз безопасности процессов аутентификации //Вопросы защиты информации.— 2014.— № 1 (104).
12. **Сабанов А.Г**. Основные процессы аутентификации // Вопросы защиты информации.— 2012.— № 3.
13. **Сабанов А.Г**. Классификация процессов аутентификации // Вопросы защиты информации.— 2013.— № 3.
14. **Сабанов А.Г**. Принципы классификации систем идентификации и аутентификации по признакам соответствия требованиям информационной безопасности //Электросвязь.— 2014.— № 2.
15. **Сабанов А.Г**. Концепция моделирования процессов аутентификации //Докл. Томского гос. ун-та систем управления и радиоэлектроники.— 2013.— № 3 (29).
16. **Сабанов А.Г**. Обзор иностранной нормативной базы по идентификации и аутентификации //Защита информации. Инсайд.— 2013.— № 4 (52).
17. **Сабанов А.Г**. Модели для исследования безопасности и надежности процессов аутентификации// Электросвязь.— 2013.— № 10.
18. **Moghissi A.A., Narland R.E., Congel F.J., Eckerman K.F**. Methodology for environmental human exposure and health risk assessment // Dyn. Exposure and Hazard Assessment Toxic chem.— Ann Arbor, Michigan, USA.— 1980.— P. 471—489.
19. **Сабанов А.Г**. Методика анализа рисков аутентификации при удаленном электронном взаимодействии. Докл. на XVI Междунар. конф. «Рускрипто-2014». Интернет-ресурс: http://www.ruscrypto.ru/accotiation/archive/rc2014/.
20. ГОСТ Р 54505—2011. Управление рисками на железнодорожном транспорте.

Получено 25.04.14