УДК 004.089

АНАЛИЗ ПРИМЕНИМОСТИ МЕТОДОВ УПРАВЛЕНИЯ РИСКАМИ 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

Оценивается возможность применения модифицированных методов управления рисками к процессам аутентификации при удаленном электронном взаимодействии. Показано, что для управления рисками аутентификации целесообразнее всего использовать методы анализа вероятных опасных событий и экономического анализа парирования угроз посредством систем защиты информации.

Ключевые слова: *аутентификация, процесс, информационная безопасность, управление рисками, удаленное электронное взаимодействие.*

Введение. Сегодня многие организации сталкиваются с необходимостью оценки риска для снижения количества опасных событий и достижения поставленных целей. Современные системы управления бизнесом все чаще включают в себя менеджмент рисков как одну из основных составляющих управления бизнесом и жизнедеятельностью предприятия. В частности, управление рисками служит основой создания и совершенствования систем информационной безопасности (ИБ). К ключевым сервисам ИБ относится аутентификация, предназначенная для подтверждения подлинности предъявленных субъектом идентификаторов и доказательства принадлежности этих идентификаторов конкретному субъекту. Развитие систем идентификации и аутентификации (СИА), как и всех сервисов безопасности, должно сопровождаться анализом рисков, объединяющим идентификацию и сравнительную оценку рисков. Анализ применимости методов оценки рисков к процессам идентификации и аутентификации пользователей при удаленном электронном взаимодействии (УЭВ) приводится в работе [1].

Результаты оценивания рисков аутентификации могут использоваться в качестве исходных данных для итеративного процесса анализа рисков и их снижения до приемлемого уровня, т.е. в процессе управления рисками.

Подходят ли методы управления рисками для процессов аутентификации? Оказалось, что для применения большей части методов управления рисками к поставленной задаче (аутентификации) требуется их модификация. Смысл модификации в том, что если в классической задаче управления рисками конечными целями анализа рисков являются обнаружение опасных событий и оценка ущерба в результате реализации этих событий конкретному активу организации, то в случае анализа рисков аутентификации требуется оценить вероятность и ущерб организации вследствие реализации опасного события безопасности функционирования подсистемы аутентификации, в частности авторизации злоумышленника под видом (с правами) легального пользователя.

Итак, целью данной работы является анализ применимости модифицированных методов управления рисками к процессам аутентификации при УЭВ. Данная статья является логическим продолжением работы [1].

Основные методы управления рисками. Рассмотрим наиболее широко используемые методы управления рисками для ИС и их применимость к анализу рисков ИБ для СИА.

Метод 1. Анализ вероятности опасного события (ВОС). Согласно [2], размер риска может быть оценен по формуле

$$R = \sum_{i=1}^{M} [P(U_i) L(U_i)],$$

где U_i — опасное событие i; $P(U_i)$ — вероятность наступления i-го опасного события; $L(U_i)$ — ущерб от наступления i-го опасного события; M — количество вероятных опасных событий.

Покажем применимость данного метода на примере опасных событий, рассмотренных в [3]. Предварительно ранжируем перечисленные опасные события на основе вероятности появления опасного события в год P и относительного значения риска $\overline{R}$ (табл. 1). Условием нормировки является

$$\overline{R} = \frac{\sum_{i=1}^{M} R_i}{\sum_{i=1}^{M} L(U_i)}.$$

Результаты ранжирования представлены на рис. 1 в виде пронумерованных точек, обозначающих номер события в табл. 1, в плоскости параметров $\{\overline{R}, (-\lg P)\}$.

Управление рисками в приведенном примере 1 может производиться как организационными, так и техническими

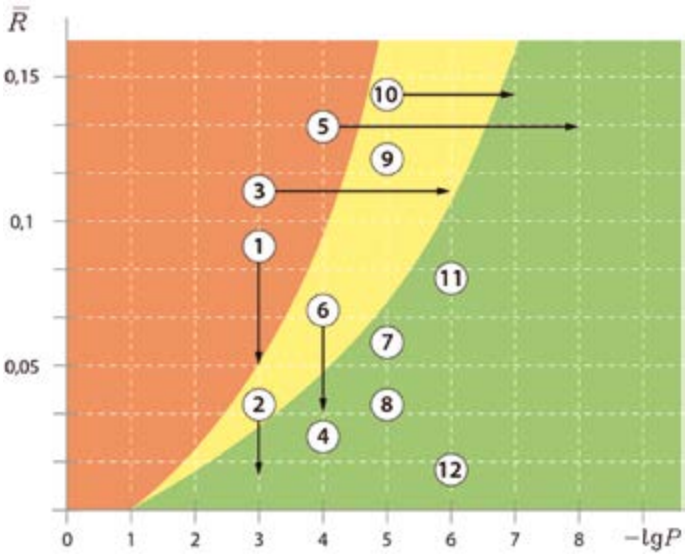

Рис. 1. **Пример ранжирования опасных событий и управления рисками**

Таблица 1. Пример ранжирования рисков аутентификации при УЭВ

ВОС	Описание опасного события	P	$\overline{R}$
1	Воздействие вредоносного ПО	10^{-3}	0,1479
2	Риск добровольной передачи носителя ключа и АИ	10^{-3}	0,1332
3	Фишинг	10^{-3}	0,1183
4	Ошибки или целенаправленные действия при смене АИ	10^{-4}	0,1109
5	Завладение злоумышленником АИ легального пользователя	10^{-4}	0,0962
6	Использование уязвимостей СИА	10^{-4}	0,0886
7	Ошибки валидации	10^{-5}	0,0769
8	Spoofing (подмена) доверенной стороны	10^{-5}	0,0695
9	Помощь инсайдера	10^{-5}	0,0563
10	Регистрация злоумышленника под видом легального пользователя	10^{-6}	0,0518
11	Атака «вход под принуждением»	10^{-6}	0,0326
12	Ошибки в принятии решения «свой–чужой»	10^{-6}	0,0178

средствами. Например, в целях снижения вероятности реализации опасного события 10 (регистрация злоумышленника под видом легального пользователя) необходим комплекс определенных мер [3, 4]. Имеется в виду повышение уровня безопасности и достоверности идентификации субъекта в процедурах регистрации нового пользователя: только личная явка субъекта в центр регистрации, тщательная проверка не менее двух действительных документов субъекта, документированная проверка предъявленных идентификаторов на актуальность в соответствующих базах данных государственных органов, использование доверенных механизмов проверки и хранения идентификаторов, строгое соблюдение регламентов по формированию учетной записи в соответствии с ролью пользователя, по выдаче аутентификатора и сертификата доступа под личную подпись.

Этот комплекс мер, согласно [3], помогает снизить вероятность реализации опасного события 10 примерно на два порядка: с 10^{-5} до 10^{-7}. Заметим, что доля населения нашей страны, активно участвующего в УЭВ, оценивается в 10^{7}. Следовательно, приведенный комплекс мер позволяет решить поставленную задачу.

Пример 2. Для снижения ВОС 3 (фишинг — подмена сайта, на который пользователю необходимо предоставить доступ) достаточно перейти с парольной аутентификации на технологию защищенного доступа SSL (Secure Socket Layer) с двусторонней взаимной аутентификацией на основе применения цифровых SSL-сертификатов на стороне сервера и клиента, что ведет к снижению вероятности подмены сайта приблизительно на два порядка (с 10^{-4} до 10^{-6}). Еще примерно на два порядка можно снизить вероятность фишинговой атаки за счет применения технологии хранения закрытого ключа и клиентского сертификата в устройстве класса SSCD (Secure Signature Creation Design — устройство генерации ключей электронной подписи [4]). Итоговое снижение ВОС в год за счет указанных мер — до 10^{-8}.

Пример 3. Рассмотрим ВОС 5 — завладение злоумышленником аутентификационной информацией (АИ) пользователя. Сама по себе кража АИ не так страшна, но весьма печальными могут оказаться последствия использования злоумышленником АИ под видом легального пользователя. Можно организационными и техническими мерами бороться за снижение вероятности появления самой кражи как таковой, однако есть и другой, более эффективный путь — снизить вероятность успешного использования АИ легального пользователя злоумышленником, применив технологию электронной подписи в качестве единственного механизма аутентификации в комбинации с устройствами аутентификации класса SSCD и политиками безопасности, ограничивающими число попыток введения неправильного PIN-кода.

В то же время снижение рисков в рассмотренных примерах может проводиться в отношении не только частоты реализации ВОС, но и размера риска. В качестве механизмов снижения рисков используются традиционные способы обеспечения доступности, целостности и конфиденциальности информации, основанные на формировании концепции информационной безопасности, моделях угроз и нарушителя, применении организационных и технических мер защиты, таких как системы защиты информации (СЗИ) и системы криптографической защиты информации (СКЗИ). При этом риски в виде точек на плоскости параметров $\{\overline{R}, (-\lg P)\}$ будут снижаться (в вертикальном направлении) до определенного уровня. Так, можно снизить риски за счет внедрения СЗИ (см. рис. 1: ВОС 1 — установка антивирусного программного обеспечения; ВОС 2 — переход на смарт-карты с технологией Match-on-Card; ВОС 6 — внедрение СЗИ в СИА). При достижении приемлемых уровней по частоте (в горизонтальном направлении) и размеру (в вертикальном направлении) идентифицированных рисков процесс управления рисками можно считать выполненным.

Если приемлемых уровней для остаточных рисков достичь не удается, необходимо подключать такие механизмы управления рисками, как уклонение от риска (ликвидация причин и/или последствий риска), ограничение (нейтрализация) риска (например, путем реализации контрмер, уменьшающих воздействие угроз безопасности), перенос риска на стороннюю организацию (страхование рисков).

К достоинствам данного метода применительно к анализу рисков аутентификации можно отнести наглядность проводимого анализа. Недостатком является необходимость большого объема предварительной работы по выявлению ВОС, зачастую в условиях отсутствия фактического материала в виде статистических данных или результатов мониторинга за достаточно продолжительный период времени. Стандарт [5] в таких случаях рекомендует воспользоваться методом экспертных оценок. Однако в целом можно рекомендовать этот метод как один из возможных для управления рисками СИА.

Метод 2. Анализ дерева уязвимостей, угроз и контрмер. В данном методе риски представляются в виде дерева уязвимостей и угроз, на которые накладываются соответствующие планируемые или применяемые контрмеры. В качестве входного параметра используется инициирующее событие и среднегодовая вероятность его реализации, в качестве выходного параметра — результирующее событие и вероятность реализации. Как правило, рассматриваемые параметры в таком анализе нормируются.

Для вероятностей P реализации событий условие нормировки можно записать в виде

$$\sum_{i=1}^{n} P_i = 1,$$

где n — число возможных состояний системы при реализации одного события.

Пример такого анализа на основе результатов работы [6] для события в виде авторизации злоумышленника в качестве легального пользователя системы приводится на рис. 2.

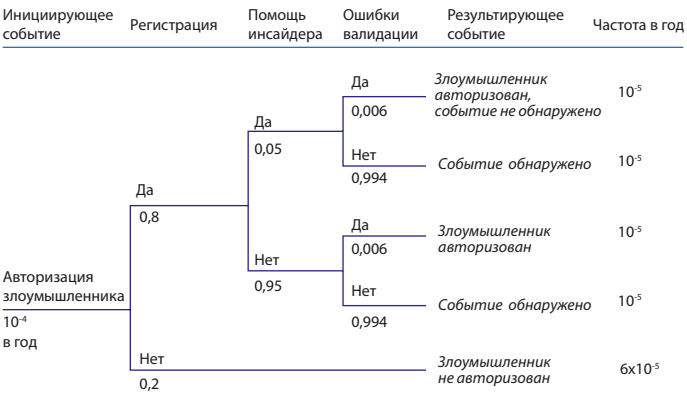

Рис. 2. **Пример анализа дерева событий**

К достоинствам метода относится наглядность цепочки событий, которые могут быть реализованы в рассматриваемой системе. Его существенный недостаток применительно к задаче аутентификации — большой объем работы по определению вероятностей событий (ветвей дерева событий). В целом метод не слишком удобен для управления рисками аутентификации при УЭВ.

Метод 3. Управление рисками попарного анализа «угроза — защита», учитывающего степень тяжести последствий от потери свойств ИБ. Метод, применимый при условии относительно полного набора выявленных угроз для конкретной рассматриваемой системы и условий ее функционирования, достаточно развит и востребован во многих сферах экономики [2], в частности, он является основой методики оценки рисков, утвержденной Банком России [7].

Суть метода — управление рисками при рассмотрении пар «угроза — степень тяжести последствий от потери свойств ИБ». В формализованном виде это выглядит следующим образом:

$$R_p = \sum_{i=1}^{k} P_p I_{pi},$$

где R_p — размер риска от реализации угрозы p; P_p — вероятность реализации угрозы p; I_{pi} — степень тяжести последствий от потери свойств ИБ, обусловленная реализацией угрозы p на свойство безопасности i; k — число свойств.

Риски R_p считаются допустимыми, если $R_p \le R_a$, где R_a — допустимый уровень рисков. В основе метода лежит анализ избыточных рисков, просуммированных для всех случаев $R_p - R_a > 0$. Пусть число избыточных рисков равно N. Тогда можно определить «обезразмеренное» среднее значение избыточного риска:

$$R_{average} = \frac{\sum_{p=1}^{N}(R_p - R_a)}{N(R_{\max} - R_a)},$$

где $R_{\max}$ — максимальное значение риска.

Величина $R_{average}$ как средний избыточный риск позволяет определить состояние ИБ в целом. Так, при близких к нулю значениях систему аутентификации можно оценить как защищенную с точки зрения ИБ, а при стремлении $R_{average}$ к единице СИА — как слабо защищенную. Одним из явных достоинств метода является возможность разбиения отрезка [0, 1] значений $R_{average}$ на интервалы, способные выполнять функции необходимого числа уровней ИБ. К его недостаткам следует отнести необходимость тщательного анализа угроз и уязвимостей СИА.

В целом данный метод может применяться для управления рисками аутентификации. При этом открытым всегда остается вопрос о доказательстве степени полноты рассматриваемых угроз. Модификацией рассматриваемого метода является оценка не только среднего избыточного риска, но и нормализованного среднего квадратичного отклонения, анализ которого более чувствителен к аномально высоким рискам и более устойчив к добавлению пар с низким избыточным риском [2].

Метод 4. Графовый метод управления рисками по изменению времени, необходимого для реализации атаки, априори считается одним из самых эффективных при проектировании и построении информационных систем и СИА как части ИС. Метод основан на базисных положениях классической теории надежности механизмов и машин. Рассмотрен в [8] применительно к задаче моделирования СИА для оценки надежности ее функционирования. Для описания процессов используются марковские и полумарковские методы анализа [9] в предположении, что условия применимости этих методов соблюдаются [10]. Суть метода в формализованном виде применительно к анализу рисков можно представить следующим образом.

Количественные способы оценки рисков базируются на формуле $R = PD$, где R — размер риска; P — вероятность наступления опасного события; D — степень тяжести последствий от его реализации.

Направленный граф состояний системы, вершины которого характеризуют вероятные состояния системы, а ребра соответствуют переходам из одного состояния в другое, позволяет оценить время перехода из i-го состояния в j-е. Одним из результатов применения графового метода является то, что он позволяет рассчитать время, необходимое для выполнения отдельных переходов из одного вероятного состояния системы в другое, в том числе оценивается вероятность перехода в опасное состояние.

В некоторых моделях время и достижимость конечной цели могут быть достаточно быстро оценены методом Петри-Маркова [11]. При введении средств защиты возможный путь и, соответственно, время, изменяются. Оценить нормализованное снижение рисков можно по формуле: $dR = 1 - t_{old}/t_{new}$, где t_{old} — время без учета введения новых СЗИ; t_{new} — время функционирования СИА с учетом введенных СЗИ. Чем ближе к единице значение dR, тем более защищенной будет система с введенной СЗИ.

Достоинством данного метода является его наглядность и универсальность; к числу недостатков следует отнести необходимость понимания процессов и умение применять, а в ряде случаев и строить математические модели СИА, что для неподготовленного специалиста не простая задача.

Метод 5. Экономический метод управления рисками. Метод заключается в повышении стоимости реализации атаки при возможном снижении стоимости установки дополнительных СЗИ для реализации контрмер. В формализованном виде ущерб SAL от однократной реализации угрозы $SAL = AV*EF$, где AV — стоимость объекта атаки; EF — относительный ущерб от успешной реализации одной атаки. Если принять в рассмотрение среднегодовую частоту реализации угрозы AWO, ожидаемый годовой ущерб

Таблица 2. Применимость методов управления рисками к аутентификации при УЭВ

Метод управления рисками	Плюсы	Минусы	Применимость
1. Анализ ВОС	Наглядность процесса управления рисками	Большой объем подготовительной работы	Да
2. Анализ дерева уязвимостей, угроз и контрмер	Наглядность цепочки событий	Неудобство в значительном объеме веток дерева событий (угроз, уязвимостей, мер)	Да, с существенными ограничениями
3. Попарный анализ «угроза–защита»	Возможность оценивать защищенность системы и вводить уровни защищенности	Необходимость рассматривать все пары. Открытым является вопрос полноты идентифицированных угроз	+/-
4. Графовый метод	Наглядность, простота алгоритма	Необходимость детально знать все процессы для построения графов	+/-
5. Экономический метод	Простота оценки эффективности внедрения СЗИ	Сложность моделирования способов реализации угроз	Да

SYL может быть оценен по формуле $SYL = SAL*AWO$. При этом значение *AWO* определяется из статистических данных о нарушениях ИБ в СИА или экспертными оценками.

Экономический эффект от реализации мер по снижению вероятности данной угрозы $ROI = (AWO*RM—CZI)/CZI$, где *RM* — коэффициент снижения риска в результате внедрения мер по снижению вероятности реализации угрозы; *CZI* — стоимость указанных мер. При положительном значении *ROI* реализация мер экономически оправданна. *ROI* представляет собой инструмент экономической оценки эффективности работы службы ИБ, целью которой является увеличение *ROI*.

Экономический эффект действий атакующего *ROA* может быть оценен по формуле $ROA = WI/(ERS + EAS)$, где *WI* — ожидаемая выгода от успешной атаки; *ERS* — затраты на атаку до внедрения СЗИ, снижающего вероятность реализации данной угрозы; *EAS* — дополнительные затраты на преодоление защитных функций СЗИ. Целью службы защиты информации является минимизация значения *ROA*, выражающаяся в снижении привлекательности ИС как объекта атак.

Достоинством данного метода является простота и прозрачность организации противодействия реализациям угроз. При этом требуется очень хорошо уметь моделировать пути реализации угроз и понимать методы противодействия.

Систематизация проведенного анализа представлена в виде итоговой табл. 2. В ней кратко показаны основные плюсы и минусы рассмотренных методов управления рисками, удобство их применения к анализу и управлению рисками аутентификации.

Из таблицы следует, что все представленные методы управления рисками применимы к анализу процессов аутентификации. Наиболее удобными инструментами управления рисками аутентификации являются методы 1 (анализ возможных опасных событий) и 5 (экономический).

Таким образом, рассмотрены все основные этапы исследования, составляющие метод анализа рисков аутентификации при УЭВ, включая один из ранее недостаточно изученных вопросов управления рисками.

Заключение. Работа посвящена исследованию применимости наиболее широко используемых методов управления рисками для анализа и управления рисками аутентификации. Изначально разрабатываемые для анализа последствий атак на актив организации, в ходе исследования они были модифицированы применительно к задаче аутентификации.

Результаты исследования могут быть полезны при проведении практических работ по управлению рисками аутентификации (проектирование и эксплуатация систем идентификации и аутентификации). В дальнейшем планируется исследовать особенности оценки надежности аутентификации для разработки методов оценки надежности и качества аутентификации при УЭВ, имея конечными целями разработку рекомендаций для внесения изменений в нормативную базу по регулированию процессов идентификации и аутентификации, а также рекомендаций для учета требований безопасности и надежности при проектировании и построении систем идентификации и аутентификации в государственных информационных системах.

ЛИТЕРАТУРА

1. **Сабанов А. Г.** Анализ применимости методов оценки рисков к процессам аутентификации при удаленном электронном взаимодействии//Электросвязь.— 2014. — № 5. — С. 44—47.
2. Управление рисками: обзор употребительных подходов.— Электронный ресурс: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/upravlenie-riskami-obzor-upotrebitelnyh-podhodov.
3. **Сабанов А. Г.** Методика идентификации рисков аутентификации //Докл. Томского гос. университета систем управления и радиоэлектроники.— 2013.— № 4 (30).— С. 136—141.
4. **Сабанов А. Г.** Многоуровневый анализ угроз безопасности процессов аутентификации //Вопросы защиты информации.— 2014.— № 1 (104).— С. 13—22.
5. ГОСТ Р ИСО/МЭК 13335—1—2006. Информационная технология. Методы и средства обеспечения безопасности. Ч. 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.
6. **Сабанов А. Г.** Методика анализа рисков аутентификации при удаленном электронном взаимодействии /Докл. на XVI Международной конференции «Рускрипто-2014».— 25—28 марта 2014.— Электронный ресурс: http://www.ruscrypto.ru/accotiation/archive/rc2014.
7. Методика оценки рисков нарушения информационной безопасности. Принята распоряжением Банка России от 11 ноября 2009 г. № Р-1190. Электронный ресурс: http://www.zakonprost.ru/content/base/part/648065.
8. **Сабанов А. Г.** Концепция моделирования процессов аутентификации //Докл. Томского гос. университета систем управления и радиоэлектроники.— 2013.— № 3 (29).— С. 71—75.
9. **Сабанов А. Г.** Модели для исследования безопасности и надежности процессов аутентификации // Электросвязь.— 2013.— № 10.— С. 38—42.
10. **Шубинский И. Б.** Структурная надежность информационных систем. Методы анализа /Ульяновск: Печатный двор, 2012.
11. **Миронова В. Г., Шелупанов А. А.** Сети Петри-Маркова как инструмент создания аналитических моделей для основных видов несанкционированного доступа в информационной системе //Докл. Томского гос. университета систем управления и радиоэлектроники.— 2012.— № 1 (25).— С. 20—24.

Получено 05.05.14