УДК 621+004.089

ОБ ОЦЕНКЕ РИСКОВ УДАЛЕННОЙ АУТЕНТИФИКАЦИИ КАК ПРОЦЕССА

А.Г. Сабанов, заместитель генерального директора ЗАО «Аладдин Р.Д.», к.т.н.; A.Sabanov@aladdin-rd.ru

Ключевые слова: *оценка рисков, удаленная аутентификация.*

Введение. Корректное формулирование требований информационной безопасности (ИБ) невозможно без предварительной оценки рисков. Переход к облачным вычислениям актуализирует необходимость обеспечения надежности и качества удаленного доступа при электронном взаимодействии. В основе создания систем управления доступом лежит решение задач идентификации и аутентификации пользователей [1]. Удаленная аутентификация является сложным процессом, состоящим из четырех основных последовательно выполняемых этапов [2, 3]: регистрации пользователя в информационной системе, установлении и проведении защищенного обмена взаимодействующих сторон, валидации электронного удостоверения претендента на успешное прохождение процедуры аутентификации и принятия решения о доступе.

При проведении анализа защищенности системы взаимодействия и выбора моделей для оценок надежности выполнения указанных этапов процесса аутентификации необходимо оценить риск. Сложность этого этапа обусловлена рядом факторов. Во-первых, существующие стандарты и методы анализа рисков разработаны для оценки в денежном выражении рисков конкретных активов, находящихся в информационной системе, а также для определения вероятности наступления рисков и

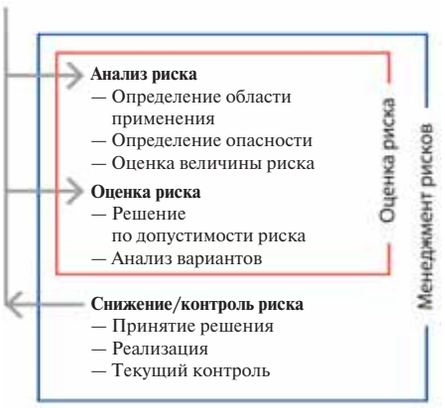

Рис. 1. **Схема анализа рисков [16]**

последствий от этого. Синтез методики оценки рисков не какого-либо актива, а сложного информационного процесса требует подходов, основанных на глубоком анализе существующих методов. Во-вторых, исследование процесса аутентификации приходится проводить для еще мало изученной сферы знаний – облачных вычислений, для которой в настоящее время стандарты не разработаны, а существующие нормативные документы имеют статус рекомендаций.

Целью данной статьи является разработка общих подходов к созданию методики оценки рисков удаленной аутентификации как процесса.

Рассмотрим сначала имеющиеся методы оценки рисков, после чего представим объект исследования и предложим собственный подход к оценке рисков.

Стандарты по анализу рисков. Международные стандарты, безусловно, сыграли ведущую роль в развитии методов и инструментария относительно молодой (всего около 20 лет) науки – анализа рисков. Из более 100 международных и 45 отечественных стандартов, касающихся проблем оценки рисков, можно выделить несколько основополагающих документов по анализу методов оценки рисков.

В группу основных источников методик и инструментов анализа рисков входят британский стандарт [4] и рекомендации по управлению рисками американского Национального института стандартов и технологий (NIST) [5]. Существенное влияние на разработку методов анализа рисков сыграли также международные стандарты [6–12]. В Российской Федерации вопросы стандартизации обеспечения безопасности информационных систем регламентируются базовыми положениями № 184-ФЗ «О техническом регулировании» [13] с изменениями [14, 15], а также переводными международными стандартами [4, 7, 16–21] и отраслевыми документами, такими как методика Банка России [22] и стандарт для железнодорожного транспорта на основе зарубежного и отечественного опыта [23].

Краткий обзор методов анализа рисков. Основные этапы оценки риска представлены на рис. 1. из которого следует, что ГОСТ Р 51901.1-2002 [16] уточняет соотношение понятий оценки риска с часто употребляемым в настоящее время понятием менеджмента рисков. Схема нашла дальнейшую детализацию в ряде документов, например в стандарте [19] для исследования отдельных информационных систем предприятия.

Для выбора той или иной методики применительно к конкретным случаям необходимо систематизировать методы оценки рисков, а при выборе методики – предварительно сформулировать требования к ней. Методы оценки рисков можно классифицировать по типу получаемых с их помощью результатов: качественные; количественные; смешанные (гибридные).

Качественные методы достаточно популярны и относительно несложны. Как правило, с их помощью можно получить оценку рисков в соответствии с простой шкалой уровней рисков, в частности низкий, средний, высокий. Как примеры качественных методов можно назвать методику и соответствующий инструментарий COBRA (первая версия разработана компанией C&A Systems Security в 1997 г. на основе стандарта [4]), методику и инструментальное средство качественной оценки рисков RA Software Tool (части 3, 4) [4, 5], а также некоторые руководства Британского национального института стандартов BSI. К категории качественных методов можно также отнести пакет FRAP (Facilitated Risk Analysis Process) [24].

Количественные методы необходимы в случаях, когда предполагаемый ущерб от реализации рисков велик, а также для того, чтобы оценить альтернативные меры по обеспечению безопасности с целью выбора наилучшей защиты.

На основе существующих методов оценки рисков созданы методики и соответствующий им инструментарий. Методики оценки рисков можно классифицировать по типу процедуры принятия решений:

- одноэтапные, которые используются, как правило, на начальной стадии развития инфраструктуры организации, когда еще не выявлены ключевые факторы, влияющие на ИБ;
- многоэтапные, с предварительной оценкой ключевых параметров. Они известны по методикам и приняты к рассмотрению: потенциальный ущерб [5]; вероятность реализации угрозы [5] или степень возможности реализации угроз ИБ [22];
- степень тяжести последствий от реализации угроз (размер ущерба) [22].

Следует заметить, что оценка рисков должна рассматриваться не как самоцель, а как определенный шаг на пути к выработке требований ИБ. Оценка риска, по международным стандартам, является итеративным и вариативным процессом, т.е. общая оценка риска должна привести к выводу о том, достигнут ли допустимый риск. Если после применения защитных мер этого не произошло, процесс оценки риска необходимо повторить. И так до тех пор, пока не будет обеспечен допустимый уровень риска. Если же риск не может быть снижен до необходимого уровня, производит-

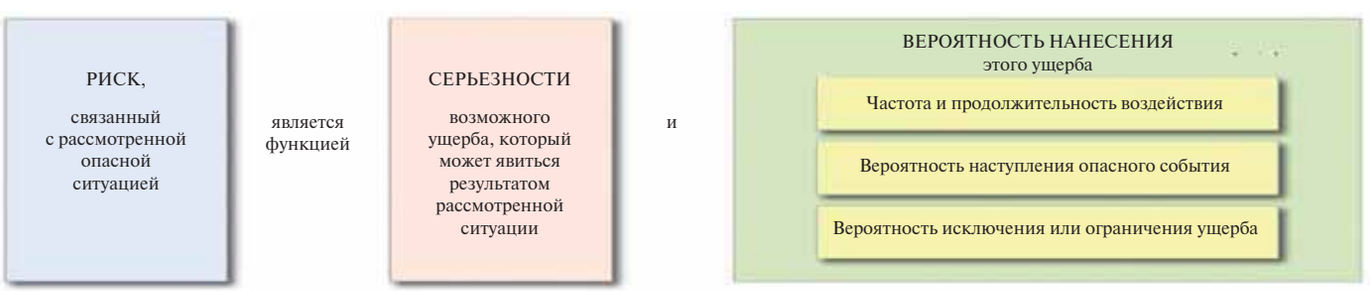

Рис. 2. **Риск, связанный с конкретным фактором**

Рис. 3. **Процесс регистрации пользователя на примере ЕСИА**

ся обработка риска информационной безопасности, т.е. осуществляются процедуры снижения (обхода или передачи риска), сохранения (принятия), предотвращения риска или переноса риска, например, путем страхования [19].

Первым этапом оценки риска является идентификация факторов опасности. Существует несколько методов анализа факторов опасности, все их можно разделить на два вида: дедуктивный и индуктивный. В дедуктивном методе предполагается конечное событие, а затем отбираются события, которые могли бы его вызвать. В индуктивном методе речь идет об отказе компонента исследуемой системы, а последующий анализ обеспечивает идентификацию событий, которые этот отказ мог бы вызвать.

Среди дедуктивных методов можно выделить метод системного анализа рисков MOSAR (Method Organized for a Systematic Analysis of Risks). Он состоит из десяти этапов. Анализируемая система рассматривается как некоторое количество подсистем, которые взаимодействуют. Используются таблицы, чтобы идентифицировать факторы опасности, опасные ситуации и опасные события. Анализ данных таблиц дает возможность выделить опасные отказы (события). Это позволяет разработать сценарии реализации рисков, которые сортируются по степени серьезности. В следующей таблице эта серьезность связывается с целями, на реализацию которых направлены меры по обеспечению безопасности, и определяются уровни эффективности технических и организационных мер. Затем меры по обеспечению безопасности включаются в логические деревья, а остаточные риски анализируются по таблице допустимости.

Еще один дедуктивный метод – FTA (Fault Tree Analysis – анализ дерева неисправностей) [16], где отправной точкой является событие, рассматриваемое как нежелательное. Этот метод, определенный также в стандарте [20], дает возможность пользователю найти целый набор критических вариантов, которые приводят к нежелательному событию. Опасные или итоговые события сначала идентифицируются, затем все сочетания отдельных отказов показываются в логическом формате дерева неисправности. Оценивая вероятности отдельных отказов и используя соответствующие арифметические операции, можно рассчитать вероятность итогового события. Влияние изменения системы на вероятность итогового события оценить легко, поэтому метод FTA упрощает исследование воздействия альтернативных мер по обеспечению безопасности.

Технологический прогноз, основанный на методе Дельфи [25], представляет собой попытку предсказать развитие той или иной технологии на длительную перспективу (до 30 лет). Разработанная впервые в 50-х годах корпорацией RAND, техника метода Дельфи впервые была использована для целей национального и отраслевого технологического прогнозирования в Японии, а впоследствии – в Германии, Франции, Великобритании, Испании, Австрии, Южной Корее. Суть метода в том, что большая группа экспертов опрашивается в несколько этапов, затем результат предыдущего этапа вместе с дополнительной информацией сообщается всем участникам. Во время третьего или четвертого этапа анонимный опрос концентрируется на тех аспектах, по которым пока никакое соглашение не достигнуто.

Среди индуктивных методов анализа факторов опасности и оценки риска следует отметить предварительный анализ факторов опасности, метод «что, если», анализ состояния и результатов отказа, моделирование неисправности в системах управления.

Назначение такого метода, как предварительный анализ факторов опасности (Preliminary Hazard Analysis), состоит в идентификации для всех этапов эксплуатационного периода факторов опасности, опасных ситуаций и опасных событий, которые могли бы привести к несчастному случаю. После идентификации возможности несчастного случая выводятся предложения о мерах по обеспечению безопасности и результат их применения.

Метод «что, если» применяется для относительно простых приложений, которые охватывают проектирование и использование оборудования. На каждом этапе задаются вопросы «что, если» и на них даются ответы, позволяющие оценить влияние отказов компонентов или методических ошибок на возникновение факторов опасности в механизме.

Цель анализа состояния и результатов отказа FMEA (Failure Mode and Effects Analysis) – оценить частоту и последствия отказа компонента. Этот метод требует более длительного времени, чем использование дерева дефектов, потому что для каждого компонента рассматривается каждый вид отказа [21, 16].

При методе моделирования неисправности в системах управления методики испытаний основаны на двух критериях: технология и сложность системы управления.

После идентификации факторов опасности должна быть выполнена оценка риска для каждого фактора опасности путем определения элементов риска. Риск, связанный с конкретной ситуацией или техническим процессом, складывается из сочетания следующих элементов (рис. 2):

1) серьезность ущерба;

2) вероятность нанесения ущерба, которая зависит от частоты и продолжительности воздействия на людей факторов опасности, вероятности наступления опасного события, возможности избежать или ограничить ущерб, связанный с техническим или человеческим фактором.

Рассмотрим каждый из элементов риска.

Серьезность ущерба помогают оценить следующие показатели:

- характер объекта, который должен быть защищен: люди, собственность или окружающая среда;
- серьезность повреждений или последствия причинения вреда здоровью: небольшая (обычно обратимый вред), значительная (обычно необратимый вред), смерть;
- степень ущерба (для каждой единицы оборудования): один человек, несколько человек.

Вероятность происхождения (нанесения) ущерба оценивается с учетом частоты и продолжительности воздействия; вероятности наступления опасного события; возможности

для предотвращения или ограничения ущерба. Практически во всех случаях на риск влияет человеческий фактор – он обязательно должен приниматься во внимание при оценке риска. Сюда включается взаимодействие с оборудованием; контакты между людьми; психологические аспекты; эргономические эффекты; способность людей осознавать риск в данной ситуации в зависимости от их опыта и квалификации. ИСО 14121 [26] рекомендует при оценке риска принимать во внимание возможность отмены мер по обеспечению безопасности или действий в обход их.

Применим результаты проведенного краткого анализа методов оценки рисков к исследованию процесса удаленной аутентификации. В качестве первого шага обратимся к объекту исследования.

Объект исследования. Описание типовой схемы аутентификации. Основываясь на рекомендациях [19], рассмотрим исследуемую систему. В общем случае процесс удаленной аутентификации может содержать четыре основных этапа: регистрация; верификация (собственно обмен защищенными сообщениями между клиентом и сервером – challenge response); валидация; принятие решения об авторизации пользователя.

Одной из самых критичных в плане безопасности и ненормируемых процедур является процедура регистрации потребителя информационных систем общего пользования (ИСОП). В отличие от закрытых (корпоративных) систем, где пользователи (сотрудники) связаны договорными отношениями (например, трудовым договором) и за их первичную идентификацию отвечает кадровая служба (идентификация проводится по нескольким предъявленным идентификаторам: паспорт, трудовая книжка, ИНН, СНИЛС, диплом об окончании вуза, диплом ученой степени, документ о повышении квалификации и т.д.), в ИСОП может обратиться любой гражданин, и не только россиянин. Для того чтобы существенно снизить вероятность мошенничества класса «маскарад», необходимо ввести строгий регламент по проверке предъявленных идентификаторов. Как минимум, можно воспользоваться опытом банков, которые перед выдачей, например, средств доступа к системе ДБО проверяют паспортные данные гражданина в нескольких базах данных.

Рассмотрим подробнее процедуру регистрации (рис. 3).

Таблица 1. Основные процессы удаленной аутентификации

Этап	Процесс	Критичные операции	Сервер (С) или клиент (К)
1	**Регистрация**		
1.1	Субъект *предъявляет* свои идентификаторы (удостоверения или ЭУ)	Ошибки ввода данных	К
1.2	ЦР *проверяет* предъявленные субъектом идентификаторы	Ошибки проверки идентификации	С
1.3	ЦР *создает* учетную запись субъекта	Ошибки ввода данных	С
1.4	ЦР *регистрирует/создает* секрет (аутентификатор) и издает ЭУ	Вероятность мала	С
1.5	ЦР *делегирует* права доступа субъекта к другим ИС	Вероятность мала	С
1.6	ЦР *выдает* секрет и ЭУ на руки субъекту	Вероятность мала	
2	**Подтверждение подлинности**		
2.1	Субъект *хранит* секрет и ЭУ	Критичная операция	К
2.2	Субъект *предъявляет* секрет и ЭУ доверяющей стороне (ДС)	Вероятность мала	К
3	**Валидация**		
3.1	ДС *проверяет* цепочку сертификатов, срок и область действия ЭУ	Вероятность мала	С
4	**Принятие решения**		
4.1	ДС *принимает* решение о результате аутентификации	Вероятность мала	С

Как видно из рисунка, исследуемая среда состоит из нескольких информационных систем с присутствием человеческого фактора во всех системах. Когда потенциальный пользователь обращается в центр регистрации (ЦР), связанный доверенными (трастовыми) отношениями с удостоверяющим центром (УЦ), уполномоченный сотрудник ЦР посылает запрос в соответствующие ведомства (ПФР, ФНС, ФМС и др.) на наличие у данного гражданина предъявленных им идентификаторов (СНИЛС, ИНН, паспортные данные) и на их действительность (наличие и совпадение в реестре) на момент проверки. Этот запрос идет через единую систему идентификации и аутентификации (ЕСИА). В случае положительных результатов проверки (и положительных ответов на запросы) ЦР создает новую учетную запись субъекта, издает его электронное удостоверение (ЭУ) и регистрирует секрет (аутентификатор) для проведения последующих сеансов аутентификации или просто фиксирует его наличие (для механизма аутентификации, реализованного путем применения технологии электронной подписи). Подробнее процедуры, составляющие процесс аутентификации, представлены в табл. 1; здесь же рассмотрена критичность (подверженность атакам) основных процедур и место, где эти процедуры производятся (на сервере или на клиентском месте).

Краткий анализ атак. Перечень возможных атак довольно широкий: прослушивание (sniffing); воспроизведение; онлайн-угадывание (например, криптографических ключей); перехват сеанса (Session Hijacking); имитация проверяющей стороны (в том числе подмена сайта – фишинг); подмена доверенного субъекта или объекта (spoofing); «человек посредине» (Man-in-the-Middle) в различных элементах системы (клавиатурный перехват, сетевой перехват и т.д.); «маскарад» – под именем легального пользователя регистрируется мошенник, который входит в систему, регистрируется и работает под чужим идентификатором; кража закрытого ключа и сертификата для доступа под чужим именем; атаки на систему управления доступом; атаки на протоколы аутентификации.

В стадии перехода к облачным вычислениям [2] особенно опасны «маскарад», «человек посредине», атаки на систему управления доступом, атаки

Таблица 2. Оценки уязвимостей и угроз процедур удаленной аутентификации

Блоки	Процесс	Уязвимости	Угрозы
1	**Регистрация**	**С**	**С**
1.1	Субъект *предъявляет* свои идентификаторы (удостоверения или ЭУ)	Н	С
1.2	ЦР *проверяет* предъявленные субъектом идентификаторы	С	В
1.3	ЦР *создает* учетную запись субъекта	Н	Н
1.4	ЦР *регистрирует/создает* секрет (аутентификатор) и *издает* ЭУ	Н	С
1.5	ЦР *делегирует* права доступа субъекта к другим ИС	Н	Н
1.6	ЦР *выдает* секрет и ЭУ на руки субъекту	Н	Н
2	**Подтверждение подлинности**	**С**	**С**
2.1	Субъект *хранит* секрет и ЭУ	С	В
2.2	Субъект *предъявляет* секрет и ЭУ доверяющей стороне (ДС)	С	С
3	**Валидация**	**Н**	**Н**
3.1	ДС *проверяет* цепочку сертификатов, срок и область действия ЭУ	Н	Н
4	**Принятие решения**	**Н**	**Н**
4.1	ДС *принимает* решение о результате аутентификации	Н	Н

инсайдеров из состава сотрудников провайдера, атаки на закрытый ключ доступа и ключ подписи, фишинг, отказ в обслуживании DoS (Denial of Service), угрозы от вредоносных программ. Другие типы атак либо не слишком часто встречаются, либо трудно осуществимы. Так, в [27] показано, что вероятность успешных атак на протоколы аутентификации чрезвычайно мала.

Методика оценки рисков аутентификации. Описание рассматриваемой сложной системы, безусловно, может быть более подробным. Степень подробности описания системы зависит от шага итераций оценки рисков [7, 8, 19].

В качестве основной цели исследования рисков по рекомендациям [19] примем разработку требований к аутентификации. За основу критериев оценки возьмем обеспечение конфиденциальности, доступности и целостности информации при организации доступа с применением исследуемых способов аутентификации. Основными задачами первого шага являются описание рассматриваемой системы, выработка целей и критериев анализа рисков и идентификация рисков.

На втором шаге выберем перечень известных методов исследования рисков для рассматриваемой системы. Учитывая основные положения по менеджменту рисков [19] и то, что аутентификация является сложным процессом, в который включены люди, аппаратное и программное обеспечение нескольких систем, сначала оценим высокоуровневые риски с помощью качественных методов.

Для проведения глубокого анализа рисков применительно к развитым информационным системам при наличии ценных для бизнеса информационных активов следует применить количественные оценки и обработать полученные риски. При необходимости предлагается провести дополнительный анализ процесса аутентификации с помощью построения дерева событий, дерева неисправностей и вида отказов [16].

Далее предлагается соотнести выявленные уязвимости с соответствующими угрозами и имеющимися статистическими данными (если они есть) по инцидентам и механизмам контроля для оценки потенциального ущерба от реализации рисков.

Пример предварительных оценок рисков. Проиллюстрируем предложенную методику для рассмотренного примера (см. табл. 1). В развитие анализа рисков на основе процессного подхода попытаемся качественно оценить угрозы и уязвимости основных процедур аутентификации. При этом учитываем, что процедуры первого блока процесса (с 1.1 по 1.6) являются разовыми, а процедуры 2.1–4.1 – многократными. Обозначим усредненные уязвимости с высокой степенью реализации (p=0,9 – 1) буквой В, со средней вероятностью ($p\approx$0,5) буквой С, с низкой вероятностью ($p\leqslant$0,1) буквой Н. Для оценки наиболее вероятных угроз примем обозначение В, для средней вероятности реализации угроз – С, для низкой вероятности – Н. Известно, что реализации методов и механизмов аутентификации достаточно многообразны. Тем не менее для рассматриваемого примера ЕСИА применяется всего два аутентификатора – пароль и закрытый ключ.

По мнению ряда экспертов, наиболее уязвимыми сегодня являются процедуры проверки предъявленных гражданином идентификаторов (существует вероятность «маскарада»), процедуры хранения секрета (наихудший случай в плане безопасности, когда роль секрета выполняет код активации, т.е. пароль) и предъявления пароля, который в общем случае могут подсмотреть, подвергнуть клавиатурным атакам и т.д., проверяющей стороне. Наиболее часто объектом угроз со стороны мошенников становятся процедуры проверки актуальности идентификаторов и хранения паролей пользователей. Результаты грубого анализа оценки уязвимостей и угроз в процедурах удаленной аутентификации собраны в табл. 2.

Представленные предварительные результаты могут служить неким ориентиром для дальнейших исследований и уточнений, в том числе с применением предложенной методики.

Заключение. В разделе 11.5.2. стандарта [28] сказано: «Строгость идентификации и аутентификации пользователя должна соответствовать важности информации, к которой будет предоставляться доступ». Этот постулат подтверждает, что предложенная типовая методика, построенная на общих принципах и нуждающаяся в адаптации к конкретной информационной системе, предназначена для информационных систем, в которых информационные активы весьма существенны для предприятий, владеющих этими активами.

Ввиду сложности процесса аутентификации представленный анализ не может претендовать на полноту. Скорее всего, как и все новое, методика исследования оценки рисков процесса аутентификации будет развиваться и уточняться, особенно в случае анализа появляющихся различных подходов к аутентификации, например при вни-

мательном рассмотрении появившихся в последние годы «облегченных» методов аутентификации (примером может служить платформа RSA Authentication Manager [29], в которой реализованы простые способы аутентификации на основе анализа рисков и больших массивов данных по истории аутентификации и поведенческих характеристик пользователей).

Проведенное исследование представляет практический интерес для предприятий и учреждений с развитой ИТ-инфраструктурой, где в последние годы весьма модно стало обсуждать риск-ориентированный метод управления информационной безопасностью. Также результаты работы могут быть использованы для анализа надежности аутентификации и качества предоставления доступа к приложениям при переходе к облачным вычислениям.

В развитие работы планируется выбор аналитической модели для анализа рисков удаленной аутентификации как процесса и продолжение работы над методикой.

ЛИТЕРАТУРА

1. **Сарбуков А., Грушо А.** Аутентификация в компьютерных системах // Системы безопасности. – 2003. – №5(53).
2. **Сабанов А.Г.** Аутентификация как составляющая Единого пространства доверия // Электросвязь. – 2012. – № 8.
3. **Сабанов А.Г.** Методы исследования надежности удаленной аутентификации // Электросвязь. – 2012. – № 10.
4. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.
5. NIST SP 800-30. July 2002. Руководство по управлению рисками.
6. AZ/NZS 4360. Risk Management Standard (с обновлениями 1999 и 2004 гг.).
7. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы обеспечения информационной безопасности. Системы менеджмента информационной безопасности. Требования.
8. ISO 13335. Международные стандарты безопасности.
9. ISO 31000:2009. Risk Management – Principles and Guidelines.
10. ISO 20000. Система управления IT-сервисами.
11. BS25999. Business Continuity.
12. ISO 22301:2012 Societal Security – Business continuity management systems – Requirements.
13. О техническом регулировании //ФЗ от 27декабря 2002 г. № 184-ФЗ.
14. О внесении изменений в ФЗ «О техническом регулировании //ФЗ от 21 июля 2011 г. № 255-ФЗ.
15. О внесении изменений в ФЗ «О техническом регулировании» //ФЗ от 30 ноября 2011 г. № 347-ФЗ.
16. ГОСТ Р 51901.1-2002. Менеджмент риска. Анализ риска технологических систем.
17. ГОСТ Р ИСО/МЭК 15408. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
18. ГОСТ Р 50992-2006. Безопасность автотранспортных средств при воздействии низких температур внешней среды. Общие технические требования.
19. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
20. ГОСТ Р 51901.13-2005 (МЭК 61025:1990). Анализ дерева неисправностей (FTA).
21. ГОСТ Р ИСО/МЭК 16085-2007. Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения.
22. Методика оценки рисков нарушения ИБ, принятая Банком России 11.11.2009 № Р-1190.
23. ГОСТ Р 54505-2011. Управление рисками на железнодорожном транспорте.
24. **Thomas R.** Peltier. Information Security Risk Analysis. – January 2001.
25. **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.
26. ISO 14121:1999 Безопасность машин. Оценка риска.
27. **Зубов А.Ю.** Математика кодов аутентификации. – М.: Гелиос АРВ, 2007.
28. ISO/IEC27002:2005. Информационные технологии. Свод правил по управлению защитой информации.
29. RSA® Authentication Manager transforms enterprise authentication by combining industry-leading SecurID with risk-based authentication for ID assurance //http://www.emc.com/about/news/press/2013/20130226-01.htm.

Получено 08.04.13