И. Г. Дровникова,
доктор технических наук, доцент

Е. С. Овчинникова

Е. А. Рогозин,
доктор технических наук, профессор

АНАЛИЗ СУЩЕСТВУЮЩИХ СПОСОБОВ И ПРОЦЕДУР ОЦЕНКИ ОПАСНОСТИ РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ И АСПЕКТЫ ИХ СОВЕРШЕНСТВОВАНИЯ

ANALYSIS OF EXISTING METHODS AND PROCEDURES FOR ASSESSING THE RISK OF NETWORK ATTACKS IN AUTOMATED SYSTEMS OF INTERNAL AFFAIRS BODIES AND ASPECTS OF THEIR IMPROVEMENT

На основе анализа методической и научно-технической литературы по проблеме информационной безопасности и нормативной базы МВД России, связанной с эксплуатацией автоматизированных систем органов внутренних дел в защищённом исполнении, в статье предложены основные направления совершенствования способов и процедур оценки опасности реализации сетевых атак в автоматизированных системах органов внутренних дел.

Based on the analysis of methodological and scientific literature on information security and normative base of the Ministry of internal Affairs of Russia related to the operation of automated systems of bodies of internal Affairs in the protected execution, the article proposes the main directions of improving the methods and procedures for assessing the danger of implementing network attacks in automated systems of internal Affairs bodies.

Введение. Опыт эксплуатации современных автоматизированных систем (АС) органов внутренних дел (ОВД) показал, что наибольший вклад в нарушение надёжности их функционирования вносят угрозы, связанные с несанкционированным доступом (НСД) к информации. Согласно ГОСТ 34.003-90 АС — это «системы, состоящие из персонала и комплекса средств автоматизации его деятельности, реализующие информационную технологию выполнения установленных функций» [1]. Безусловно, АС ОВД следует отнести к системам критического применения, выход из строя которых ведёт к значительным информационным и финансовым потерям, следовательно, вопросы, связанные с защитой информации (ЗИ) в АС на объектах информатизации ОВД, являются весьма актуальными. Их актуальность основывается на основных положениях Доктрины информационной безопасности (ИБ), в которой отмечается необходимость как повышения защищённости критической информационной структуры и устойчивости её функционирования, так и развития механизмов обнаружения, защиты и предупреждения информационных угроз [2].

Анализ международных и отраслевых стандартов Российской Федерации по ИБ АС [3, 4], Руководящих документов Федеральной службы по техническому и экспорт-

ному контролю (ФСТЭК) России [5—8], Руководящих документов Государственной технической комиссии при Президенте Российской Федерации [9—13], а также ведомственных нормативных актов по вопросам ЗИ на объектах информатизации ОВД [14] показал, что оценка эффективности функционирования систем и средств ЗИ на этапе эксплуатации АС и разработка адекватных существующим угрозам перспективных образцов этих систем является одним из важнейших моментов в процессе эксплуатации АС ОВД в защищённом исполнении. Это приводит к необходимости анализа угроз, связанных с НСД к информационному ресурсу АС ОВД. Последствием реализации указанных угроз является финансовый и другой ущерб, нанесённый в результате нарушения конфиденциальности, целостности или доступности информации, что, в свою очередь, приводит к нарушению функционирования АС ОВД по прямому назначению (хранение, обработка и передача служебной информации).

При рассмотрении вопроса функционирования АС ОВД в защищённом исполнении определяющее значение имеют информационные угрозы НСД, которые реализуются через удалённое взаимодействие с объектом воздействия (сетевые атаки) [15, 16].

Процесс проектирования и функционирования защищённых АС ОВД осуществляется, как правило, с учётом использования в них технологии межсетевого взаимодействия, реализованной в Internet, и стека протоколов TCP/IP. Таким образом, в распределённых сетях может быть реализовано большинство атак, характерных для глобальной сети. Территориальная распределённость, влекущая за собой реализацию значительного количества сетевых атак, является одной из важных особенностей функционирования АС ОВД в защищённом исполнении [17].

Общей методологией анализа сетевых атак является системный подход, который согласно [18, 19] может быть сведён к решению следующих задач для АС на объектах информатизации ОВД: определению возможных источников атак, выявлению уязвимостей программно-аппаратного обеспечения АС ОВД, оцениванию возможностей реализации атак в АС ОВД, оцениванию опасности атак и формированию в результате перечня актуальных атак для данной АС ОВД.

Таким образом, обеспечение необходимой степени защищённости АС ОВД для эффективного функционирования в условиях сетевых атак предполагает реализацию процедуры оценивания опасности атак и формирования на этой основе частной модели актуальных атак для конкретной АС на объекте информатизации ОВД, что, в свою очередь, требует разработки адекватных показателей и методики оценки опасности их реализации.

Теоретический анализ. Необходимость развития количественных методов оценки опасности реализации сетевых атак в современных АС ОВД объясняется как требованиями повышения обоснованности принятия решений по ЗИ, так и дальнейшими перспективами формализации и оперативного управления процессами ЗИ, разработки АС поддержки принятия решений по ЗИ на объектах информатизации ОВД и т.д.

Опасность сетевых атак оценивается по размеру информационного риска [19].

С термином «риск» обычно связывается некая качественная или количественная характеристика, определяющая потенциальную степень опасности некоторого рассматриваемого действия.

В [20, 21] даётся определение риска как «влияния неопределённостей на процесс достижения поставленных целей». При этом подчеркивается, что:

- цели могут иметь различные аспекты: финансовые, аспекты, связанные со здоровьем, безопасностью и внешней средой, и могут устанавливаться на разных уровнях: на стратегическом уровне, в масштабах организации, на уровне проекта, продукта и процесса;

- риск часто характеризуется ссылкой на потенциальные события, последствия или их комбинацию, а также на то, как они могут влиять на достижение целей;

- риск часто выражается в терминах комбинации последствий события или изменения обстоятельств и их вероятности [20].

В [22] риск трактуется как «вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учётом тяжести этого вреда».

В [23] приводится определение риска чрезвычайной ситуации как «меры опасности чрезвычайной ситуации, сочетающей вероятность возникновения чрезвычайной ситуации и её последствий».

В [24] риск также понимается как «сочетание вероятности нанесения ущерба и тяжести этого ущерба» Данное определение соответствует тому, что понимается под риском в большинстве публикаций.

Таким образом, информационный риск в условиях сетевых атак следует рассматривать как сочетание двух характеристик: величины возможного ущерба от реализации атак и оценки возможности этой реализации (т.е. нанесения ущерба).

Анализ методической и научно-технической литературы по проблеме оценивания опасности реализации угроз ИБ позволяет констатировать, что в настоящее время отсутствует единство в выделении основных показателей опасности угрозы.

Так, в [25] предлагаются следующие показатели опасности угрозы: уровень защищённости АС и потенциал нарушителя, необходимый для реализации данной угрозы ИБ в заданной АС (для оценки возможности реализации угрозы); наивысшие значения величины каждого вида возможного ущерба, связанного с нарушением конфиденциальности, целостности, доступности каждого вида информации (для оценки итоговой величины возможного ущерба).

В [26] при оценивании опасности угрозы персональным данным (ПДн) и определении актуальных угроз их безопасности в АС ПДн применяются два показателя: коэффициент реализуемости угрозы и вербальный показатель опасности для рассматриваемой АС ПДн.

В [18, 27] оценивание угрозы ИБ производится на основе использования комплексного показателя — коэффициента опасности угрозы K_{thu}, представляющего собой свертку коэффициента опасности несанкционированного действия K_g и вероятности реализации угрозы $P_{thu}(t)$:

$$K_{thu} = K_g \cdot P_{th\,u}(t), \tag{1}$$

где K_g определяется в виде отношения максимального к предельно допустимому размеру нанесённого ущерба (применительно к общему объёму информационного ресурса, для которого данное несанкционированное действие может быть реализовано):

$$K_g = \frac{\bar{u}}{u_{пр}}. \tag{2}$$

Для корректного выбора параметров в процессе осуществления количественного анализа риска атакуемой АС в [28] используется схема воздействия на систему (рис. 1), где: $p_{вi}$, $p_{рi}$ — вероятности возникновения и реализации i-й атаки соответственно, $p_{уij}$ — вероятность нанесения ущерба вида j реализацией i-й атаки, u_j — величина нанесённого ущерба вида j. Представленные четыре параметра являются показателями опасности i-й атаки.

Разнообразие подлежащих учёту факторов, вариантов последствий от реализации сетевых атак обусловливает то, что в настоящее время отсутствует официально признан-

ная методика количественной оценки возможного ущерба от их реализации [18], а следовательно, и методика количественной оценки опасности реализации сетевых атак в АС ОВД.

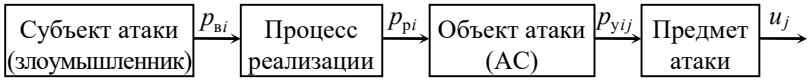

Рис. 1. Схема сетевой атаки на АС и соответствующие её элементам параметры

При оценивании опасности реализации угроз из множества используемых в настоящее время подходов можно выделить четыре наиболее популярных (табл. 1).

Таблица 1

Основные подходы, используемые при оценивании опасности реализации угроз

Подход	Характеристика подхода
1	Основан на экспертном методе оценки, представленном в методических документах ФСТЭК России [25, 26]
2	Основан на методе оппозиционных (полярных) шкал [18, 27]
3	Основан на балльном (табличном) методе оценки [28]
4	Основан на математическом моделировании процессов реализации угроз [19]

Изложенная в [25] методика определения угроз ИБ в АС широко используется для выявления, оценки угроз и разработки их моделей в ходе создания АС и периодического пересмотра (переоценки) угроз в ходе эксплуатации систем. Она применяется, как правило, не изолированно, а в совокупности с банком данных угроз ИБ (ubi.fstec.ru), разработанным ФСТЭК России, а также с базовыми и типовыми моделями угроз ИБ в АС различных классов и типов, формируемых ФСТЭК России. Сущность используемого подхода к оцениванию опасности реализации угроз ИБ заключается в том, что идентифицированная *j*-я угроза нейтрализуется (блокируется), если она является актуальной ($УИБ_j^A$) для рассматриваемой системы. Следовательно, в любой АС, имеющей определённые структурно-функциональные характеристики и особенности функционирования, вероятна (возможна) реализация угрозы нарушителем, обладающим необходимым потенциалом. Негативным последствием реализации рассматриваемой угрозы является нанесённый ущерб от нарушения конфиденциальности, целостности или доступности информации:

$$УИБ_j^A = [\text{вероятность } (P_j) \text{ (возможность } (Y_j)) \text{ реализации угрозы; степень ущерба } (X_j)]. \quad (3)$$

В случае отсутствия статистических данных для расчёта P_j определение актуальности *j*-й угрозы ИБ основывается на оценке Y_j:

$$Y_j = [\text{уровень защищённости АС } (Y_1); \text{ потенциал нарушителя } (Y_2)]. \quad (4)$$

Для $УИБ_j^A$ вводятся три вербальные градации (низкая, средняя и высокая) в соответствии с экспертными оценками P_j (Y_j) и X_j.

В методике определения актуальных угроз безопасности ПДн [26] предлагаются два показателя для оценки возможности реализации исследуемой угрозы в АС ПДн — степень исходной защищённости компьютерной системы и частота (вероятность) реализации угрозы.

Степень исходной защищённости системы представляется в виде обобщённого показателя, зависящего как от технических, так и от эксплуатационных её характеристик. Он определяется исходя из результатов положительных решений по уровням защищённости. Каждой степени исходной защищённости (высокой, средней, низкой) ставится в соответствие целочисленный коэффициент Y_1, принимающий значения 0; 5 или 10.

Частота (вероятность) реализации угрозы представляется в виде определяемого экспертным путём показателя, измеряющего степень вероятности реализации конкретной угрозы безопасности ПДн конкретной системы в имеющихся условиях. Задаются четыре вербальные градации частоты (вероятности) реализации угрозы с учётом объективных предпосылок её реализации. Каждой градации (маловероятная, низкая, средняя, высокая вероятность) ставится в соответствие целочисленный коэффициент Y_2, принимающий значения 0; 2; 5 или 10.

Коэффициент реализуемости угрозы находится по формуле:

$$Y = (Y_1 + Y_2)/20. \quad (5)$$

При $0 \le Y \le 0{,}3$ возможность реализации угрозы считается низкой, при $0{,}3 < Y \le 0{,}6$ — средней, при $0{,}6 < Y \le 0{,}8$ — высокой, при $Y > 0{,}8$ — очень высокой.

Оценка опасности реализации угрозы (низкая, средняя, высокая) производится с учётом степени негативных последствий для субъектов ПДн на основе определения вербального показателя опасности для конкретной АС ПДн путём опроса экспертов.

Изложенный в [18, 27] подход, используемый при осуществлении количественной оценки величины ущерба и опасности реализации угроз ИБ, базируется на применении оппозиционных (полярных) шкал. Суть его заключается в том, что для каждого вида ущерба указываются, как минимум, два полярных значения на шкале, трактуемые в качестве противоположных результатов оценки величины ущерба (незаметный ущерб — неприемлемый ущерб). Далее строятся метрические шкалы, в которых максимально возможный (либо неприемлемый ущерб) задаётся в качестве максимального значения, а отсутствие такого ущерба (либо незаметный ущерб) — в качестве минимального.

Приведение оценок разнородных ущербов к единой шкале оценок производится путём построения базовой вербальной шкалы, установления её соответствия каждой из шкал оценок разнородных ущербов, а также нормированной решётке, представляющей собой отрезок [0;1], на который проецируется вербальная шкала (рис. 2).

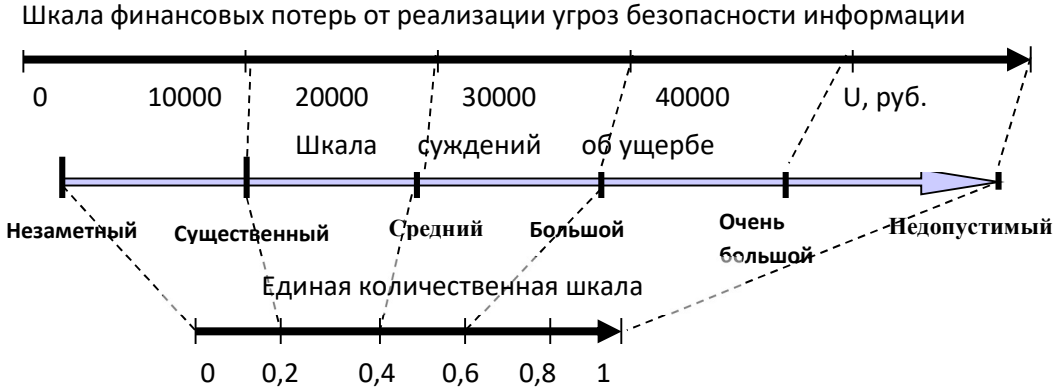

Рис. 2. Пример приведения разнородных шкал к единой количественной шкале

Опасность реализации угрозы рассчитывается по формуле (1), где $K_g \le 1$, и определяется на нормированной полярной шкале с помощью экспертных оценок.

Балльный (табличный) метод оценки опасности реализации угроз представляет собой реализацию последовательности этапов: 1-й этап — опрос экспертов, 2-й этап —

обработка полученных результатов опроса, 3-й этап — перевод обработанных результатов опроса в баллы, 4-й этап — интерпретация балльной оценки по вербальной шкале в виде суждений об опасности [28].

Указанный метод достаточно популярен и реализован в ряде международных стандартов и программных продуктов, таких как стандарт ISO/IEC 27002:2005-2013 [29] и его инструментарий — программный продукт COBRA или программный продукт, реализующий метод CRAMM (CCTA Risk Analysis & Management Method — метод анализа и контроля рисков Центрального агентства по компьютерам и телекоммуникациям Великобритании), программный продукт Risk Watch и др. В настоящее время наиболее широко применяемым является метод CRAMM.

Математическое моделирование процессов реализации угроз ИБ проводится с использованием аналитических методов теории массового обслуживания и её составной части — теории потоков, теории вероятностей, марковских и полумарковских процессов, а также методов теории сетей Петри — Маркова [19].

Поскольку сетевые атаки имеют вероятностный характер и изменяются в процессе функционирования АС ОВД [17], в качестве базовой аналитической модели описания атаки применяется вероятностная модель атак на АС, в которой для выражения объективных соотношений используются термины теории вероятностей и математической статистики [28].

Так как в современных АС ОВД протекает множество параллельных процессов, выполнение которых влияет на протекание сетевых атак [17], то реализация атак на данные АС является сложным динамическим процессом. Учитывая данный факт, описание процесса реализации рассматриваемых сетевых атак целесообразно осуществлять с использованием моделей, построенных на сетях Петри — Маркова (основанных на теории сетей Петри и полумарковских процессах), что позволит определять как вероятностно-временные, так и статистические характеристики при исследовании реализации параллельных процессов [30].

Однако каждая атака реализуется по-своему и требует разработки своей базовой аналитической модели. Из-за этого, во-первых, приемлемый по полноте набор таких моделей отсутствует, во-вторых, спектр сетевых атак постоянно расширяется, что вынуждает создавать всё новые модели. А это не только затруднительно, но и приводит к значительным сложностям их практического применения, так как обусловливает необходимость, наряду с созданием приемлемых описательных моделей, разрабатывать программные средства моделирования процессов их реализации, поскольку без автоматизации расчётов количественно оценить возможности реализации угроз крайне сложно. С учётом изложенного следует подчеркнуть, что четвёртый подход сегодня только начинает развиваться. В то же время можно с уверенностью констатировать, что математическое моделирование параллельных процессов на основе аппарата сетей Петри — Маркова позволит существенно повысить адекватность оценки возможностей реализации сетевых атак в компьютерных системах. Поскольку в настоящее время проведение количественной оценки размеров нанесённого ущерба весьма проблематично (данная задача относится к слабо формализуемым), то при оценивании опасности угрозы ИБ размеры возможного ущерба либо считаются неприемлемыми, либо осуществляется переход к их качественным оценкам [18, 19].

Очевидным общим недостатком рассмотренных показателей и методик является их сравнительно низкая пригодность для построения точных количественных оценок опасности реализации сетевых атак на этапах всего жизненного цикла защищённых АС при их эксплуатации на объектах информатизации ОВД.

Заключение. Таким образом, анализ методической и научно-технической литературы по проблеме ИБ, а также нормативной базы МВД России, регламентирующей эксплуатацию АС ОВД в защищённом исполнении, выявил ряд вопросов, требующих

безотлагательного решения с целью повышения защищённости АС на объектах информатизации ОВД:

1) существующие показатели опасности реализации угрозы не отражают реальные угрозы удалённого доступа, реализуемые посредством сетевых атак, в АС на объектах информатизации ОВД;

2) существующие методики оценки опасности реализации сетевых атак в АС не учитывают особенности, которые возникают при эксплуатации АС ОВД в защищённом исполнении (в частности, распределённая обработка больших объёмов служебной информации, влекущая значительное количество параллельно реализуемых сетевых атак);

3) не содержится чётких количественных требований к оценке опасности реализации сетевых атак в АС на объектах информатизации ОВД (существующие методики количественной оценки являются неточными и нуждаются в доработке в соответствии с требованиями ГОСТ Р 51583-2014 [3] и приказа МВД России от 14.03.2012 № 169 [14]);

4) в недостаточном объёме разработано математическое обеспечение оценки опасности реализации сетевых атак в АС ОВД, что требует существенной доработки;

5) имеющиеся нормативно-распорядительные документы по ЗИ на объектах информатизации ОВД нуждаются в доработке с учётом требований современной международной и отечественной нормативной документации, регламентирующей разработку и эксплуатацию АС ОВД в защищённом исполнении.

ЛИТЕРАТУРА

1. ГОСТ 34.003-90. Автоматизированные системы. Термины и определения [Электронный ресурс]. — URL: http://docs.cntd.ru/document/1200006979_(дата обращения: 10.10.2019).
2. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 № 646 // СПС «КонсультантПлюс» (дата обращения: 10.10.2019).
3. ГОСТ Р 51583-2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении [Электронный ресурс]. — URL: http://docs.cntd.ru/document/1200108858 (дата обращения: 11.10.2019).
4. ГОСТР ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2: Функциональные компоненты безопасности [Электронный ресурс]. — URL: http://docs.cntd.ru/document/ 1200105710 (дата обращения: 18.10.2019).
5. ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс]. — URL: https: //fstec.ru/tekhnicheskaya-zashchita-informatsii (дата обращения 14.10.2019).
6. ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации [Электронный ресурс]. — URL: http://fstec.ru/component/ attachments/download/299 (дата обращения: 18.10.2019).
7. ФСТЭК РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [Электронный ресурс]. — URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379 (дата обращения: 11.10.2019).
8. ФСТЭК РФ. Руководящий документ. Базовая модель угроз безопасности персо-

нальных данных при их обработке в информационных системах персональных данных (выписка) [Электронный ресурс]. — URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379 (дата обращения: 11.10.2019).

9. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 30 июня 1992 года. Защита от несанкционированного доступа к информации. Термины и определения [Электронный ресурс]. — URL: https://fstec.ru/component/attachments/download/298 (дата обращения: 10.10.2019).

10. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 года. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс]. — URL: http://files.stroyinf.ru/Data2/1/4293809/4293809157.htm (дата обращения: 24.09.2019).

11. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 года. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники // СПС «КонсультантПлюс» (дата обращения: 24.09.2019).

12. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 года. Защита от несанкционированного доступа к информации. Часть 1: Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей [Электронный ресурс]. — URL: http://meganorm.ru/ Index2/1/4293808/4293808514.htm (дата обращения: 24.09.2019).

13. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 года. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации // СПС «КонсультантПлюс» (дата обращения: 24.09.2019).

14. Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года : приказ МВД России от 14.03.2012 № 169 [Электронный ресурс]. — URL: http://policemagazine.ru/forum/showthread.php?t=3663 (дата обращения: 21.10.2019).

15. Радько Н. М., , Скобелев И. О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удалённого и непосредственного доступа. — М. : РадиоСофт, 2010. — 232 с.

16. Методы и средства оценки защищённости автоматизированных систем органов внутренних дел : монография / А. Д. Попов [и др.]. — Воронеж : ВИ МВД России, 2017. — 88 с.

17. Попов А. Д. Модели и алгоритмы оценки эффективности систем защиты информации от несанкционированного доступа с учётом их временных характеристик в автоматизированных системах органов внутренних дел : дис. ... канд. техн. наук : 05.13.19 / Попов Антон Дмитриевич. — Воронеж, 2018. — 163 с.

18. Язов Ю. К., Соловьёв С. В. Организация защиты информации в информационных системах от несанкционированного доступа: монография. — Воронеж : Кварта, 2018. — 588 с.

19. Язов Ю. К., Соловьёв С. В. Защита информации в информационных системах от несанкционированного доступа: пособие. — Воронеж : Кварта, 2015. — 440 с.

20. ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения [Электронный ресурс]. — URL: http://docs.cntd.ru/document/

1200075565 (дата обращения: 10.10.2019).

21. ГОСТ Р 51897-2011. Национальный стандарт Российской Федерации. Менеджмент риска. Термины и определения [Электронный ресурс]. — URL: http://docs.cntd.ru (дата обращения: 10.10.2019).

22. О техническом регулировании : федеральный закон от 27.12.2002 № 184-ФЗ // СПС «КонсультантПлюс» (дата обращения: 21.10.2019).

23. ГОСТ Р 22.0.02-2016. Национальный стандарт Российской Федерации. Безопасность в чрезвычайных ситуациях. Термины и определения [Электронный ресурс]. — URL: http://docs.cntd.ru/document/1200139176 (дата обращения: 21.10.2019).

24. ГОСТ Р 51898-2002. Национальный стандарт Российской Федерации. Аспекты безопасности. Правила включения в стандарты [Электронный ресурс]. — URL: http://docs.cntd.ru/document/1200030314 (дата обращения: 21.10.2019).

25. ФСТЭК России. Методический документ. Методика определения угроз безопасности информации в информационных системах [Электронный ресурс]. — URL: http://https://fstec.ru/component/attachments/download/812 (дата обращения: 21.10.2019).

26. ФСТЭК России. Методический документ. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]. — URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380 (дата обращения: 18.10.2019).

27. Радько Н. М., Язов Ю. К., Корнеева Н. Н. Проникновения в операционную среду компьютера: модели злоумышленного удалённого доступа : учеб. пособие / Н. М. Радько. — Воронеж : Воронежский государственный технический университет, 2013. — 265 с.

28. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. — М.: Компания АйТи ; ДМК Пресс, 2004. — 384 с.

29. Стандарт ISO/IEC 27002:2005-2013 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью [Электронный ресурс]. — URL: http: // docs.cntd.ru

30. Игнатьев В. М., Ларкин Е. В. Сети Петри — Маркова. — Тула : ТулГУ, 1997. — 163 с.