ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2022-49-3-91-103 Оригинальная статья /Original Paper

Методический подход к количественной оценке рисков реализации угроз несанкционированного доступа к информационному ресурсу автоматизированных систем органов внутренних дел

Т.В. Мещерякова[1], Е.А. Рогозин[1], А.О. Ефимов[1], В.Р. Романова[1], С.А. Коноваленко[2]
[1] Воронежский институт МВД России,
[1]394065, г. Воронеж, пр. Патриотов, 53, Россия,
[2]Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
[2]350063, г. Краснодар, ул. Красина, 4, Россия

Резюме. Цель. Характерной особенностью современного этапа развития сферы информатизации органов внутренних дел (ОВД) является значительный рост объема и многообразия видов служебной информации ограниченного распространения, хранящейся, обрабатываемой и передаваемой в автоматизированных системах (АС). Это порождает возникновение большого количества и расширение номенклатуры угроз безопасности информации, в первую очередь – угроз, связанных с несанкционированным доступом (НСД) к информационному ресурсу АС ОВД, и вызывает необходимость совершенствования имеющихся способов борьбы с данным видом преступлений для обеспечения информационной безопасности объектов информатизации ОВД. Для получения информации, позволяющей оценивать степень угроз, необходимо провести количественную оценку рисков. **Метод.** Метод оценки рисков реализации угроз несанкционированного доступа к информационному ресурсу АС ОВД и получения данных в количественном представлении основывается на использовании методов математического моделирования. Преимущество количественной оценки по сравнению с качественной оценкой заключается в возможности сопоставления рисков с конечным результатом, который можно представить в денежном эквиваленте, и дальнейшего использования при оценивании вероятности реализации информационных угроз и расчете нанесенного ущерба. **Результат.** Предложен методический подход к количественной оценке рисков реализации угроз НСД к информационному ресурсу АС ОВД, позволяющий оценивать уровень защищенности служебной информации. **Вывод.** Предложенный методический подход к количественной оценке рисков реализации угроз НСД к информационному ресурсу АС ОВД дает наглядное представление в денежном эквиваленте по объектам оценки (ущербу, затратам). Данные расчеты можно использовать при обосновании требований к уровню защищенности АС ОВД при их разработке и эксплуатации.

Ключевые слова: автоматизированная система, риск, несанкционированный доступ, угроза, защита информации

Для цитирования: Т.В. Мещерякова, Е.А. Рогозин, А.О. Ефимов, В.Р. Романова, С.А. Коноваленко. Методический подход к количественной оценке рисков реализации угроз несанкционированного доступа к информационному ресурсу автоматизированных систем органов внутренних дел. Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(3):91-103. DOI:10.21822/2073-6185-2022-49-3-91-103

Methodical approach to quantitative assessment of the risks of the implementation of threats unauthorized access to an information resource automated systems of internal affairs bodies

T.V. Meshcheryakova[1], E.A. Rogozin[1], A.O. Efimov[1], V.R. Romanova[1], S.A. Konovalenko[2]
[1]Voronezh Institute of the Ministry of Internal Affairs of Russia,
[1]53 Patriotov Str., Voronezh 394065, Russia,
[2] General of the Army S.M. Shtemenko Krasnodar Higher Military School,
4 Krasina Str., Krasnodar 2350063, Russia

Abstract. Objective. A characteristic feature of the current stage of development of the sphere of informatization of internal affairs bodies (OVD) is a significant increase in the volume and variety of types of service information of limited distribution, stored, processed and transmitted in automated systems (AS). This gives rise to the emergence of a large number and expansion of the range of threats to information security, primarily threats associated with unauthorized access (UAS) to the information resource of the ATS AS, and necessitates the improvement of existing methods to combat this type of crime in order to ensure the information security of objects of informatization of ATS. To obtain information that allows assessing the degree of threats, it is necessary to conduct a quantitative risk assessment. **Method.** The method for assessing the risks of implementing threats of unauthorized access to the information resource of the ATS AS and obtaining data in a quantitative representation is based on the use of mathematical modeling methods. The advantage of a quantitative assessment compared to a qualitative assessment is the ability to compare risks with the final result, which can be represented in monetary terms, and further use in assessing the likelihood of information threats and calculating the damage caused. **Result.** A methodical approach to the quantitative assessment of the risks of the implementation of UA threats to the information resource of the ATS AS is proposed, which makes it possible to assess the level of security of service information. **Conclusion.** The proposed methodological approach to quantitative assessment of the risks of the implementation of UA threats to the information resource of the ATS AS provides a visual representation in monetary terms of the objects of assessment (damage, costs). These calculations can be used to justify the requirements for the level of security of ATS ASs during their development and operation.

Keywords: automated system, risk, unauthorized access, threat, information security

For citation: T.V. Meshcheryakova, E.A. Rogozin, A.O. Efimov, V.R. Romanova, S.A. Konovalenko. Methodical approach to quantitative assessment of the risks of the implementation of threats unauthorized access to an information resource automated systems of internal affairs bodies. Herald of the Daghestan State Technical University. Technical Science. 2022; 49(3):91-103. DOI:10.21822/2073-6185-2022-49-3-91-103

Введение. В эпоху развития информационных технологий особое внимание уделяется обеспечению необходимого уровня защищенности служебной информации ограниченного распространения, циркулирующей на объектах информатизации ОВД, от угроз, связанных с НСД к информационным ресурсам. Согласно руководящему документу Федеральной службы по техническому и экспортному контролю (ФСТЭК) России «Защита от несанкционированного доступа к информации. Термины и определения» НСД представляет собой доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники, или АС [1]. Ссылаясь на ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения», под информационной угрозой понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [2].

Для минимизации угроз и проведения оценки рисков их реализации в АС ОВД необходимо определить вид потенциальных угроз:

- угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программно-математического воздействия).

Постановка задачи. Настоящее время характеризуется бурным ростом информационных технологий в различных сферах деятельности, что в полной мере относится и к сфере ин-

форматизации ОВД. С каждым днем увеличивается объем служебной информации ограниченного распространения, являющейся основным ресурсом для решения поставленных оперативно-служебных задач.

В МВД РФ обеспечение высокого уровня защищенности АС министерского назначения является приоритетным направлением ОВД, эксплуатирующих систему. Основой при определении требований к защищенности АС ОВД являются международные и стандарты РФ по информационной безопасности (ИБ) АС, такие как, ГОСТ Р 51583-2014, ГОСТ ИСО/МЭК-Р 15408-2013. Так же на объектах информатизации ОВД нашли применение приказы МВД России, приказ от 14.03.2012 №169. Проведенный анализ нормативных актов показал, что одной из главенствующих задач при эксплуатации защищенных АС ОВД является количественная оценка эффективности систем защиты информации (ЗИ) при разработке и эксплуатации АС ОВД, после которой можно выбрать наилучшую систему защиты.

Важнейшим этапом построения любой АС ОВД должен стать анализ рисков реализации угроз ИБ, который поможет верно определить условия и факторы, влияющие на нарушение целостности, конфиденциальности и доступности циркулирующей в системе информации, и оценить потенциальную опасность информационных угроз. Грамотная оценка уязвимостей АС ОВД и рисков реализации возможных угроз НСД к информационному ресурсу послужит основой для оптимизации принятия решений по защите служебной информации ограниченного распространения с учетом необходимых затрат.

Методы исследования. Под защищенностью АС ОВД согласно ГОСТ Р 50922-2006 понимается возможность предотвращать НСД, при этом система должна сохранять возможность функционирования по своему прямому назначению [2]. Проведение оценки защищенности предназначено для определения степени адекватности реализованных в ней систем и средств ЗИ, имеющихся в данной среде функционирования рискам [2].

В Руководящем документе ФСТЭК 2004 [7] определена общая методика проведения оценки защищенности АС ОВД.

Процесс оценки защищенности АС ОВД состоит из подготовки к проведению и непосредственно проведения оценки защищенности АС ОВД [7].

Проведение оценки защищенности АС ОВД предусматривает подготовку исходных данных, необходимых для оценки, включающих: документирование описания АС ОВД; категорирование АС ОВД; идентификацию угроз безопасности для АС ОВД; определение показателей, по которым будет проводиться оценка АС ОВД; определение состава участников проведения оценки защищенности; предоставление исходных данных для оценки уровня защищенности АС [7].

Практическая оценка защищенности АС ОВД включает в себя четыре этапа [7].

Первый является предварительным этапом, который связан с анализом достаточности материалов для оценки, оценкой предъявленных к АС ОВД требований безопасности информации, определением способов оценки.

Вторым этапом является оценка безопасности АС ОВД.

На третьем этапе выполняется подтверждение соответствия АС ОВД требованиям безопасности информации.

Четвертым этапом оценки защищенности является поддержка доверия к безопасности АС ОВД.

Методика оценки защищенности АС ОВД согласно требованиям Руководящего документа Гостехкомиссии от 19.06.2002 №187 предназначена для оценки параметров безопасности продуктов и систем информационных технологий [8]. Методический документ ФСТЭК 2015 года «Методика выявления НСД в АС» определяет показатели, характеризующие проектную защищенность информационной системы [9].

Рассмотренные выше нормативные правовые акты показывают, что оценка защищенно-

сти АС ОВД строится на основе определенного класса защиты АС ОВД. Также рассмотренные документы не предусматривают проведение количественной оценки защищенности информации.

Для выбора мер и средств защиты информации необходимо грамотно и в полной мере оценить возможные риски нарушения информационной безопасности АС ОВД от реализации угроз НСД.

Существуют различные способы оценки рисков реализации угроз НСД к информационному ресурсу АС ОВД, которые можно объединить в два основных взаимно дополняющих друг друга вида – качественная оценка и количественная оценка.

Главной задачей качественной оценки рисков является выявление факторов риска, этапов работы АС ОВД, при выполнении которых возникает риск, установление потенциальных областей риска, после чего определяются все возможные риски, требующие устранения для оптимальной работы АС ОВД. Качественная оценка включает в себя также рассмотрение методологического подхода к количественной оценке приемлемого уровня риска. При необходимости получения конечных данных, выраженных в денежном эквиваленте, временных ресурсах, процентах или иной количественной информации, применяется количественная оценка рисков реализации угроз НСД к информационному ресурсу АС ОВД, позволяющая получить конкретные значения объектов оценки рисков путем проведения аналитических расчетов.

Количественная оценка подразумевает присвоение конкретных значений для получения выходной информации в количественном представлении. Алгоритмы, обеспечивающие получение выходных значений, должны быть четкими и понятными. Объектом оценки могут стать такие данные, как вероятность наступления угрозы, размер ущерба от реализации угрозы, стоимость мер защиты информации в АС ОВД и др.

Основная цель обоих методов состоит в выявлении предполагаемых угроз НСД к информационному ресурсу, а также выбор эффективных мер и средств защиты служебной информации в АС ОВД. Каждый метод оценки рисков имеет свои преимущества и недостатки.

Использование количественного метода позволяет рассчитывать стоимость ущерба от реализации угроз, однако он более трудоемок по сравнению с качественным методом. Проведение качественной оценки рисков реализации угроз НСД к информационному ресурсу АС ОВД сократит время оценивания, однако повысит степень субъективизма полученного результата. Использование качественного метода не подразумевает под собой конкретных выходных данных, что не даст наглядного понимания размеров причиненного ущерба. Для получения более точного выходного значения объекты оценки должны содержать реальные данные и быть представленными в удобном для анализа виде.

Обсуждение результатов. Для оценки риска реализации любой угрозы информационной безопасности АС ОВД необходимо определить и описать компоненты (факторы риска), используемые в качестве входных данных, способные повлечь за собой нарушение конфиденциальности информации, ее целостности и доступности.

Типовые факторы риска включают в себя: угрозы; уязвимости; негативное влияние; вероятность; предварительные условия. Основные элементы процесса оценивания информационной безопасности объекта информатизации представлены на рис. 1.

Источником угрозы нарушения безопасности информации может стать как целенаправленное действие с целью завладения служебной информацией ограниченного распространения и дальнейшего ее использования, так и ненамеренное действие, причиной которого является недоработка (неверная эксплуатация) АС ОВД, позволяющая инсайдеру воспользоваться уязвимостью.

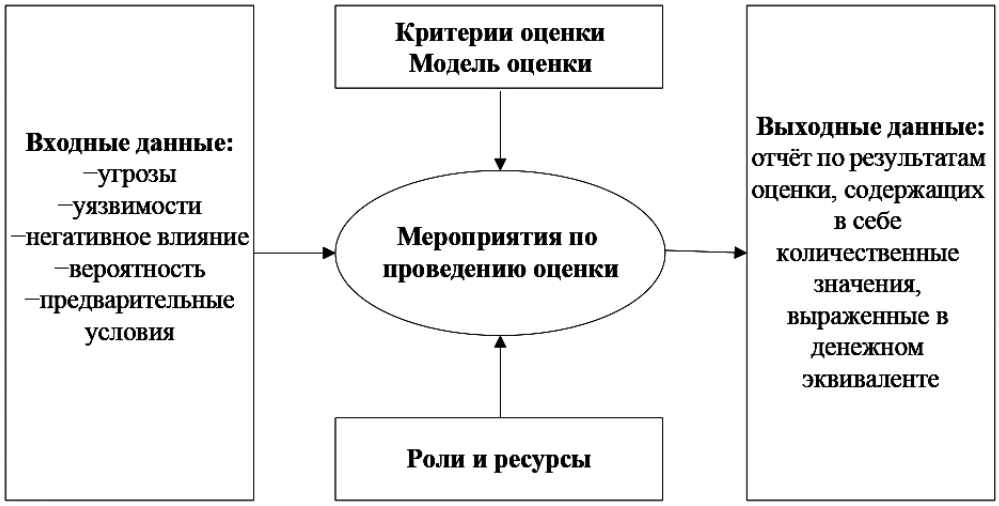

Рис. 1.Основные элементы проведения оценки информационной безопасности объекта информатизации

Fig. 1. The main elements of the information security assessment of the informatization object

От точности построения модели рисков, от грамотного описания всех факторов риска зависит детализация определения событий угроз. Детальное рассмотрение различных моделей рисков позволит построить сценарии угроз, включающие совокупность нескольких событий угроз, в результате которых наступает негативный эффект, относящийся к определенному источнику угрозы или к их совокупности.

Уязвимостью считается недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (ая) может быть использован (а) для реализации угроз безопасности информации [3]. Степенью опасности уязвимости приятно считать меру (сравнительную величину), характеризующую подверженность АС уязвимости и ее влияние на нарушение свойств безопасности информации (конфиденциальности, целостности, доступности) [3].

В большинстве своем, уязвимости возникают из-за применения намеренных действий по получению служебной информации, либо ненамеренных действий, связанных с недоработкой или неправильной эксплуатацией АС ОВД. При этом важно учитывать не только эволюцию информационной среды, но и совершенствование способов деструктивного воздействия злоумышленника, что требует обеспечения соответствующей защиты информационных ресурсов АС ОВД.

Негативное влияние события угрозы подразумевает под собой размер ущерба, возникающего от реализации угроз НСД, например получение доступа к информации, ее изменение, утеря и недоступность.

Явным образом определяют: процесс, используемый для определения негативного влияния; предположения, используемые для определения негативного влияния; источники и методы получения информации о негативном влиянии; логическое обоснование, использованное для определения негативного влияния.

Вероятность возникновения информационной угрозы, связанной с НСД, является важным фактором при оценке рисков. Она подразумевает под собой рассчитываемый аналитически фактор риска, связанный с эксплуатацией определенной уязвимости (совокупности уязвимостей), определенной угрозой с учетом вероятности причинения угрозой реального ущерба.

На основании вышесказанного входные данные можно описать в виде логической структуры, которая является основой для получения интересующей информации, выраженной в количественном представлении: источник угрозы с определенной долей вероятности провоцирует определенную угрозу, которая эксплуатирует уязвимость, следствием чего является создание негативного влияния, порождающего риск. Мероприятия по проведению оценки рисков

реализации угроз НСД к информационному ресурсу АС ОВД могут быть осуществлены с помощью внутреннего и внешнего аудита. Аудит информационной безопасности подразумевает под собой систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению информационной безопасности и установлению степени выполнения в организации критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации [6]. Различные типы аудита представлены в табл. 1.

Таблица 1. Различные типы аудита информационной безопасности
Table 1. Different types of information security audit

Аудит первой стороны First party audit	Аудит второй стороны Second party audit	Аудит третьей стороны Third party audit
Внутренний аудит Internal audit	Аудит внешнего поставщика External supplier audit	Аудит для сертификации и/или аккредитации Audit for certification and/or accreditation
	Аудит другой внешней заинтересованной стороны Audit of another external stakeholder	Аудит соблюдения законодательства, нормативных правовых требований и аналогичных целей Audit of compliance with legislation, regulatory legal requirements and similar purposes

Необходимыми условиями обеспечения достоверной оценки информационной безопасности при проведении аудита являются: использование доверенного процесса аудита; использование наиболее достоверных источников оценки; определение объема выборки с учетом заданной достоверности оценки; учет факторов, влияющих на аудиторский риск, с целью его снижения. Доверенный процесс аудита информационной безопасности должен отвечать требованиям принятого нормативного документа, описывающего данный процесс.

Критерии оценки, служащие критическими элементами для измерения объекта оценки должны быть представлены в удобном для анализа виде с целью получения на выходе данных, отражающих степень риска реализации угроз НСД к информационному ресурсу АС ОВД в числовом виде.

Основой модели оценки процесса аудита информационной безопасности служит совокупность показателей, являющихся базовыми для сбора объективных данных. С помощью данных, полученных в результате анализа входных параметров, можно последовательно сформировать суждения по оценке анализа, а также повысить эффективность полученных результатов.

Показатели позволяют оценивать степень реализации процессов объекта оценки. Модель оценки процесса аудита с наибольшим числом входных параметров обеспечивает более глубокий анализ, что позволит получить максимально приближенный к действительности результат. Однако такой анализ требует значительного увеличения ресурсов.

Каждый процесс характеризуется входными параметрами, выходными данными (результатом), управляющими воздействиями и ресурсами. Состояние любого процесса отображается совокупностью параметров процесса оценки, входных параметров, параметров управления, параметров ресурсов и выходных параметров.

Для проведения оценки функционирования процессов каждый из них должен быть представлен совокупностью параметров, требуемых для функционирования процессов в соответствии с их назначением. При соблюдении всех условий на выходе можно получить данные, которые помогут: оценить в количественном выражении потенциальный ущерб от реализации каждой угрозы; определить вероятность реализации каждой из угроз информационной безопасности АС ОВД; определить общий потенциальный ущерб от каждой угрозы за контрольный период; провести анализ полученных данных по ущербу для каждой угрозы.

Анализ угроз безопасности информации имеет целью установление того, каким способом существует возможность нарушения конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) или доступности (блокирование) информации, содержащейся в АС ОВД. Результат воздействия НСД показан на рис. 2:

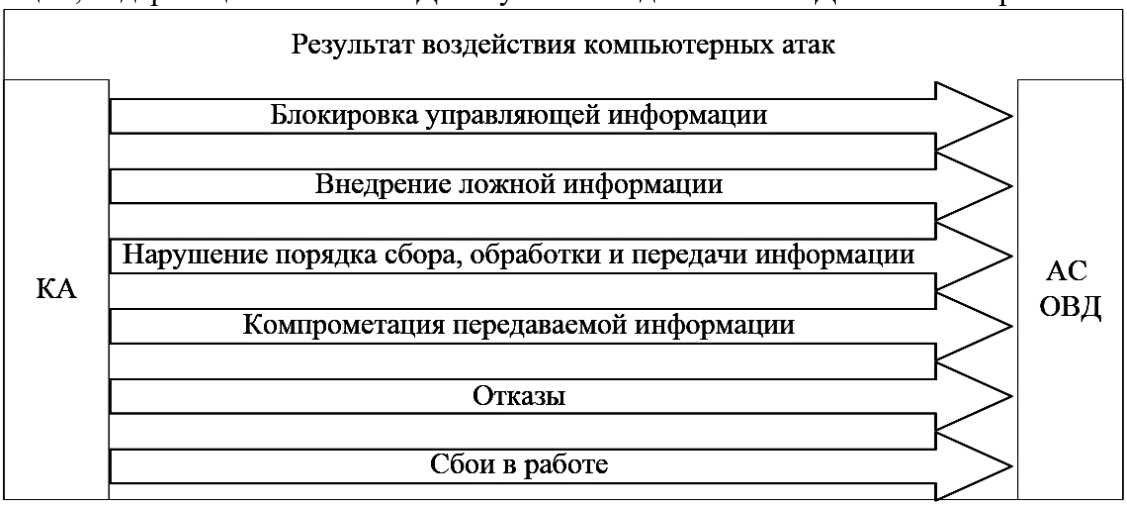

Рис. 2. Результат воздействия НСД на информационный ресурс АС ОВД
Fig. 2. The result of the impact of NSD on the information resource of the ATS AS

По способу воздействия компьютерные атаки делятся на сетевые и протокольные. По целевому назначению основные типы компьютерных атак представлены на рис. 3 [10]:

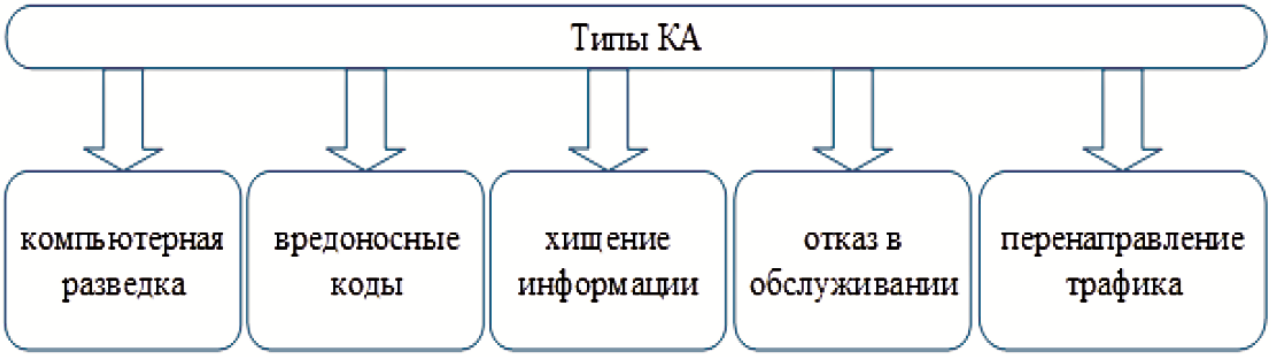

Рис. 3. Типы компьютерных атак на АС ОВД
Fig. 3. Types of computer attacks on ATS automated systems

На основе проведенного анализа угроз безопасности информации АС ОВД наиболее актуальным способом в современном мире является осуществление противником компьютерных атак, воздействие которых направлено на элементы системы, поэтому дальнейшее исследование необходимо проводить исходя из условий воздействия на АС ОВД компьютерных атак.

С целью обеспечения ЗИ необходимо использовать механизмы защиты, под эффективностью применения которых понимается повышение защищенности АС ОВД за счет решения ряда частных задач. Исходя из множества задач, решаемых с целью обеспечения требуемого уровня защищенности информации, необходимо построить методику и алгоритм их решения в виде комплексной оценки защищенности. Для этого строится следующий пошаговый алгоритм действий.

Шаг 1. Задаются исходные данные, начальные и конечные условия:

- количество элементов АС ОВД, подверженных воздействию компьютерных атак – N;
- наличие реализованных средств ЗИ;
- описание угроз безопасности информации, уязвимостей и реализованных средств ЗИ в АС ОВД.

Шаг 2. В соответствии с установленными средствами ЗИ, осуществляющими ограничи-

тельные действия злоумышленнику, целью противоправных действий которого являются нарушение функционирования АС ОВД, определяются типы возможных инцидентов, возникающих в результате действия злоумышленника, и на основе имеющихся уязвимостей, определяется связь уязвимостей АС ОВД, инцидентов и необходимых мер ЗИ.

Шаг 3. В соответствии с возможностями злоумышленника, возникающими в результате их действий инцидентами, выбирается комплекс организационных и технических мероприятий по предотвращению неправомерных действий злоумышленником, соответствующий каждому отдельно взятому инциденту [11].

Шаг 4. Определяется критерий эффективности для оценки защищенности АС ОВД.

$$J = \frac{\min}{\max}\begin{Bmatrix} Q \\ E \\ R \\ O \\ D \end{Bmatrix}, \qquad (1)$$

где Q – эффективность АС ОВД; E – точность АС ОВД; R – надежность АС ОВД; O – быстродействие; D – затраты ресурсов.

Ввиду невозможности определения универсального критерия оценки эффективности в связи с различными условиями эксплуатации АС ОВД, а также неопределенностью, связанной с действиями внешней среды целесообразно учитывать ряд особенностей при его формировании. Так, предлагается общий подход к построению критерия, который основывается на следующих предположениях:

1. В каждом конкретном случае эксплуатации АС ОВД необходимо предавать конкретный вес соответствующему критерию. Для различных условий эксплуатации АС ОВД и воздействий внешний среды экспертным путем определены соответствующие решаемым задачам значения критериев методом анализа иерархий (табл. 2);

Таблица 2. Значения критериев
Table 2. Criteria values

№ п/п	Q	E	R	O	D
1	0,3	0,08	0,1	0,27	0,25
2	0,16	0,32	0,17	0,29	0,06
3	0,14	0,08	0,11	0,36	0,31
4	0,42	0,27	0,23	-	0,08

2. В условиях неопределенности действия злоумышленника на АС ОВД следует распределить показатели по группам и формировать их исходя их цели выполнения задач.

Исходя их вышесказанного, для оценки защищенности АС ОВД целесообразно в качестве основных критериев выбрать быстродействие и затраты ресурсов, характеризующих с одной стороны скорость выполнения необходимых для оценки защищенности операций, а с другой стороны, затраченные на это ресурсы.

Правильный выбор оптимальных значений критериев позволит гарантированно осуществить оценку защищенности АС ОВД в условиях отсутствия полной достоверной информации о предполагаемых действиях злоумышленника.

Поиск оптимального соотношения критериев осуществляется по следующей схеме:

$$\left.\begin{matrix} O \to \max \\ D = D_{opt} \end{matrix}\right\} \; при\; D_{opt} \to \min, \qquad (2)$$

где D^{opt} – допустимые затраты ресурсов.

Шаг 5. Определяется вектор ограничений, характеризующийся условиями применимости методики. Так как основными функциями эксплуатируемой АС ОВД являются учет, хранение, передача, обработка, циркулирующей в каналах связи информации и предоставление оператору донесений о виде и форме, полученной в результате ее обработки, то в работе в качестве области возможных действий противника Ω предлагается рассмотрение компьютерных атак.

$$A_{\min}(t) \le A(t) \le A_{\min}(t), \quad (3)$$

$$A(t) \in \Omega, \quad (4)$$

где $A(t)$ – воздействие компьютерных атак.

Шаг 6. Определяется вектор возможных действий, обеспечивающих гарантированную стратегию поиска рационального использования ресурсов в зависимости от угроз противника.

$$u(t) \in V, \quad (5)$$

где V – множество всех возможных действий, направленных против воздействия злоумышленника.

Шаг 7. В качестве показателей, характеризующих процесс оценки защищенности АС ОВД, предложено выбирать вероятности нейтрализации НСД.

$$P_{защ} = 1 - \prod_{m=1}^{k} P_{преод_m}, \quad (6)$$

где k – общее количество имеющихся механизмов защиты, которые нужно нейтрализовать злоумышленнику; $P_{преод}$ – вероятность преодоления НСД средств защиты.

В случае экспоненциальной аппроксимации имеющихся параметров

$$P_{преод_m} = \frac{\overline{t_{fm}}}{\overline{t_{fm}} + \overline{t_{um}}}, \quad (7)$$

где $\overline{t_{fm}}$ – среднее время между соседними изменениями параметров m-ого механизма защиты;

$\overline{t_{um}}$ – среднее время НСД m-ого механизма защиты.

Поэтому, при определении эффективности СЗИ, прежде всего, нужно найти среднее время между соседними изменениями характеристик m-ого СЗИ и ($\overline{t_{um}}$) НСД.

Для этого использовались профильные модели механизмов – в виде «Вредоносных кодов» при НСД «Ransomware», воздействующих на ППЭВМ (сервер), с установленными на них антивирусной СЗИ и метод топологических изменений случайных сетей.

Профильная модель компьютерной атаки:

- получение пакета сообщения на порт ППЭВМ (сервера), зараженными вредоносным кодом «Ransomware» за $\overline{t_{получ}}$ с функцией распределения $W(t)$;
- дефрагментация сетевой картой ППЭВМ (сервера) указанного пакета за среднее время $\overline{t_{дефр}}$ с функцией распределения $M(t)$;
- запуск сканера антивируса в оперативной памяти ППЭВМ (сервера) имеющегося пакета за $\overline{t_{пров}}$ с функцией распределения $L(t)$;
- с вероятностью P_I преодоление антивирусной системы вредоносным кодом «Ransomware» за среднее время $\overline{t_{скан}}$ с функцией распределения $B(t)$;

– заражение ППЭВМ за среднее время $\overline{t_{зар}}$ с функцией распределения *O(t).*

Если пакет заблокирован, то с вероятностью (1-P_I) противник повторно направляет запрос за среднее время $\overline{t_{блок}}$ с функцией распределения *Z(t).*

Требуется определить интегральную функцию распределения вероятности $F(t)$ и среднее время $\bar{T}$ преодоления антивирусной системы.

Описанный выше процесс представлен в виде стохастической сети (рис. 4):

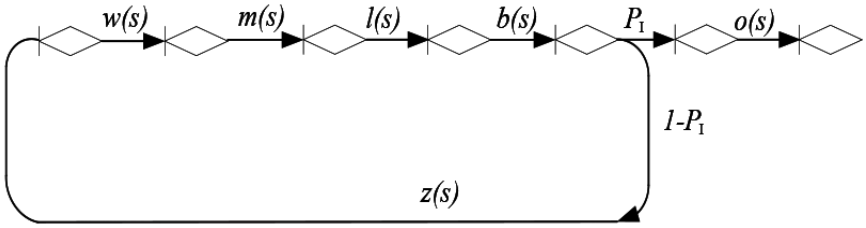

Рис. 4. Стохастическая сеть компьютерной атаки вида «Вредоносные коды» при реализации способом «Ransomware»
Fig. 4. Stochastic network of a computer attack of the "Malious codes" type when implemented using the "Ransomware" method

Расчетные выражения для интегральной функции распределения вероятности и среднего времени реализации компьютерной атаки [12],

$$F(t)=\sum_{k=1}^{6}\frac{w\cdot m\cdot l\cdot b\cdot P_I\cdot o\cdot(z+s_k)}{\varphi'(s_k)}\cdot\frac{1-\exp[s_k t]}{-s_k}, \quad (8)$$

$$\bar{T}=\sum_{k=1}^{6}\frac{w\cdot m\cdot l\cdot b\cdot P_I\cdot o\cdot(z+s_k)}{\varphi'(s_k)}\cdot\frac{1}{(-s_k)^2}. \quad (9)$$

Результаты расчетов вероятностно-временных характеристик представлены на рис. 5, 6. В качестве исходных данных используются следующие значения:

$\overline{t_{получ}}$= 8 мин, $\overline{t_{дефр}}$=8 мин, $\overline{t_{пров}}$= 8 мин, $\overline{t_{скан}}$= 8 мин, $\overline{t_{блок}}$= 8 мин, $\overline{t_{повт}}$= 1 мин, P_I= 0,1…0,9.

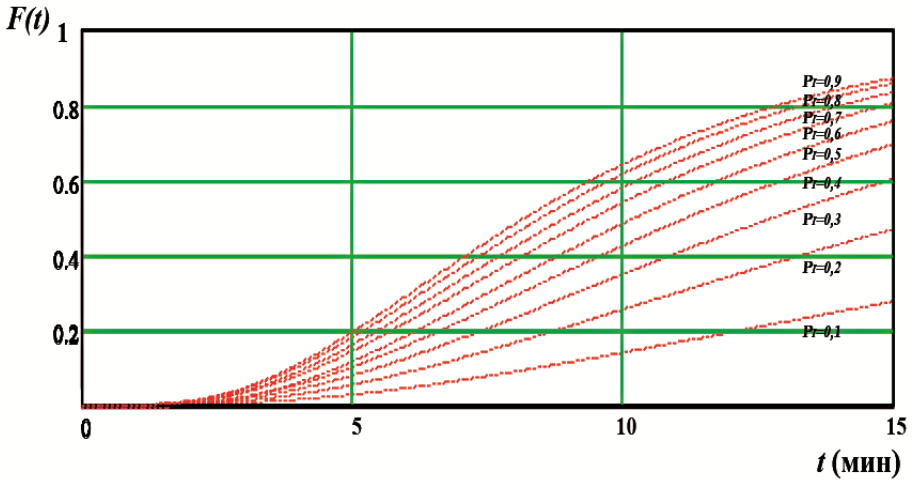

Рис. 5. Зависимость интегральной функции распределения вероятности от времени преодоления антивирусной системы
Fig. 5. Dependence of the integral probability distribution function on the time to overcome the anti-virus system

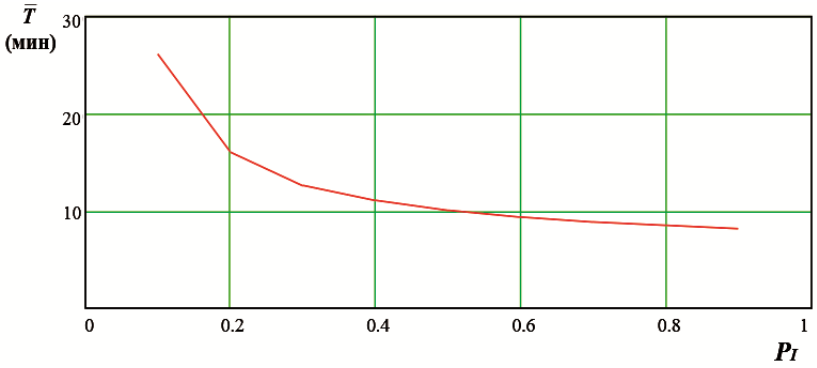

Рис. 6. Зависимость среднего времени от вероятности преодоления антивирусной системы
Fig. 6. Dependence of the average time on the probability of overcoming the anti-virus system

Шаг 8. Для определения уровня защищенности АС ОВД, значение только коэффициента защищенности недостаточно, поэтому исходя из полученной оценки защищенности на основе вероятностей преодоления злоумышленником средств защиты, реализованных в АС, предлагается использовать вербально-числовую шкалу Харрингтона (табл. 3).

Таблица 3. Вербально-числовая шкала Харрингтона
Table 3. Harrington Verbal Number Scale

№ п/п	Содержательное описание градаций Meaningful description of gradations	Числовое значение Numeric value
1	Очень высокая Very high	08-1,0
2	Высокая High	0,64-0,8
3	Средняя Medium	0,37-0,64
4	Низкая Low	0,2-0,37
5	Очень низкая Very low	0,0-0,2

Таким образом, разработанная методика оценки защищенности позволяет определить угрозы и обосновать соответствующие им меры защиты; оценивает НСД для элементов АС ОВД и ее системы защиты в условиях информационного противоборства.

Вывод. По итогам применения предложенного методического подхода к количественной оценке рисков реализации угроз НСД к информационному ресурсу АС ОВД определяются актуальные атаки, реализация которых может подвергнуть систему нарушению безопасности обрабатываемой в ней служебной информации ограниченного распространения (нарушению ее конфиденциальности, целостности или доступности), а также нарушению функционирования самой системы.

Полученные систематизированные результаты по оценке рисков реализации информационных угроз НСД для конкретной АС ОВД выражаются в количественном представлении (числовом эквиваленте).

Обеспечение безопасного, устойчивого и надежного функционирования современных объектов информатизации ОВД является актуальной и сложной задачей, решение которой видится в проведении количественной оценки рисков реализации угроз НСД к информационному ресурсу АС ОВД в соответствии с требованиями действующей методической документации ФСТЭК России, а также директив, приказов и инструкций МВД России.

В отличие от существующих в настоящее время методов, основанных на экспертных оценках рисков, осуществление их количественной оценки позволит проводить исследования в динамическом (временном) диапазоне и разрабатывать конкретные рекомендации по повышению уровня защищенности объектов информатизации.

Библиографический список:

1. ФСТЭК РФ. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения.
2. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения // М.: Федеральное агентство по техническому регулированию и метрологии. 2006. 12 с.
3. ГОСТ Р 56546–2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. 2016. 8с.
4. ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
5. ГОСТ Р 15408–2013. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий // М.: Стандартинформ. 2014. 152 с.
6. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. 2008. 22с.
7. Руководящий документ. Безопасность информационных технологий. Концепция оценки соответствия автоматизированных систем требованиям безопасности информации: утв. ФСТЭК России 2004 г.
8. Руководящий документ Гостехкомиссии. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий: утв. Приказом Гостехкомиссии от 19.06.2002 №187.
9. Методика определения угроз безопасности информации в информационных системах: утв. ФСТЭК России 2015 г.
10. Коцыняк М.А., Кулешов И.А., Кудрявцев А.М., Лаута О.С. Киберустойчивость ИТКС. СПб, 2015 г.
11. Требования о защите информации, содержащейся в информационных системах общего пользования: утв. приказом ФСТЭК России от 31 августа 2010 г. №489
12. Бешелев С.Д., Гурвич Ф.Г. Математико-статистические методы экспертных оценок. – М.: Статистика,1980. – 263 с.
13. Мочалов Д.А., Вольф В.А., Романова В.Р., Рогозин Е.А., Калач А.В. Анализ существующих угроз внешнего нарушителя к информационному ресурсу веб-серверов в автоматизированных системах вооруженных сил российской федерации // Вестник Воронежского института ФСИН России №1–2022. С. 68-75.
14. Коноваленко С.А., Королев И.Д. Выявление уязвимостей информационных систем посредством комбинированного метода анализа параметрических данных, определяемых системами мониторинга вычислительных сетей // Альманах современной науки и образования №11-2016. С.60-66.
15. Система защиты информации от несанкционированного доступа «Страж NT». Описание применения. URL: http://www.rubinteh.ru/public/opis30.pdf (дата обращения: 23.06.2022).
16. Yang N. Modeling and quantitatively predicting software security based on stochastic Petri nets / N. Yang, H. Yu, Z. Qian, H. Sun // Mathematical and Computer Modelling. — 2012. — Vol. 55. — Issues 1–2. — pp.102–112.
17. Klaic A. Conceptual Modeling of Information Systems within the Information Security Policies / A. Klaic, M. Golub // Journal of Economics / Business and Management. — 2013. — vol. 1. — Issue 4. — pp. 371–376.
18. Nazareth D. System dynamics model for information security management / D. Nazareth, J. Choi // Information & Management. — 2015. — vol. 52. — Issue 1. — pp. 123–134.
19. Complex Event Processing Modeling by Prioritized Colored Petri Nets / H. Macià [and others] // IEEE Access. — 2016. — vol 4. — pp. 7425–7439.
20. Nikishin K. Implementation of time-triggered ethernet using colored Petri NET / K. Nikishin, N. Konnov, D. Pashchenko // International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). —2017. — pp. 1–5.
21. Korniyenko B.Y. Design and research of mathematical model for information security system in computer network / B.Y. Korniyenko, L.P. Galata // Science-Based Technologies. — 2017. — vol. 34. — Issue 2. — pp. 114–118.
22. White S.C. Comparison of Security Models: Attack Graphs Versus Petri Nets / S.C. White, S.S. Sarvestani // Advances in Computers. — 2014. — vol. 94. — pp. 1–24.
23. Jasiul B. Detection and Modeling of Cyber Attacks with Petri Nets / B. Jasiul, M. Szpyrka, J. Sliwa // Entropy. — 2014. — vol. 16. — Issue 12. — pp. 6602–6623.

References:

1. FSTEC of the Russian Federation. Guidance document. Protection against unauthorized access to information. Terms and definitions. (In Russ)
2. GOST R 50922-2006. Information protection. Basic terms and definition. Moscow: *Federal Agency for Technical Regulation and Metrology.* 2006.12 K. (In Russ)
3. GOST R 56546-2015. Information protection. Communications of information systems. Classification of information systems. 2016; 8. (In Russ)
4. FSTEC of the Russian Federation. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and information security requirements. (In Russ)
5. GOST R 15408-2013. Methods and means of ensuring security. Criteria for assessing the security of information technologies Moscow: *Standartinform*. 2014;152. (In Russ)
6. GOST R 53114-2008. Information protection. Ensuring information security in the organization. Basic terms and definitions. 2008; 22. (In Russ)
7. Guidance document. Information technology security. The concept of assessing the compliance of automated systems with information security requirements: approved by FSTEC of Russia 2004. (In Russ)
8. The guiding document of the State Technical Commission. Information technology security. Criteria for assessing the security of information technologies: approved. By Order of the State Technical Commission No. 187 dated 06/19/2002. (In Russ)

9. Methodology for determining the risk of information security in information systems: approved by FSTEC of Russia 2015 (In Russ)
10. Kotsynyak M. A., Kuleshov I. A., Kudryavtsev A.M., Lauta O. S. Cyberstability of ITCS. St. Petersburg, 2015(In Russ)
11. Requirements for the protection of information contained in public information systems: approved by Order No. 489 of the FSTEC of Russia dated August 31, 2010. (In Russ)
12. Beshelev S. D., Gurvich F. G. Mathematical and statistical methods of expert assessments. *M.: Statistics*, 1980; 263. (In Russ)
13. Mochalov D. A., Wolf V. A., Romanova V. R., Rogozin E. A., Kalach A.V. Analysis of existing threats of an external intruder to the information resource of web servers in automated systems of the Armed forces of the Russian Federation. *Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia* 2022; 1: 68-75. (In Russ)
14. Konovalenko S.A., Korolev I.D. Identification of vulnerabilities of information systems by means of a combined method of analysis of parametric data determined by monitoring systems of computer networks. *Almanac of modern science and education* 2016; 11:60-66. (In Russ)
15. Information protection system from unauthorized access "Sentinel NT". Description of the application. Stole: http://www.rubinteh.ru/public/opis30.pdf (accessed: 06/23/2022). (In Russ)
16. Yang N. Modeling and quantitatively predicting software security based on stochastic Petri Nets / N. Yang, H. yu, Z. kIan, H. Sun. *Mathematical and Computer Modeling*. 2012; 55: 1-2:102-112.
17. Klaik A. Conceptual Modeling of Information Systems within the Information Security Policies / A. Klaik, M. Golob / *Journal of Economics. Business and Management.* 2013; l (4): 371-376.
18. Nazareth D. System dynamics model for Information security management / D. Nazareth, J. Choi. *Information & Management.* 2015; 52 (1): 123-134.
19. Complex Event Processing Modeling would be Prioritized Colored Petri Nets / H. Makià [and others]. *IEEE Access*. 2016; 4: 7425-7439.
20. Nikishin K., N. Konnov, D. Pashchenko. Implementation of time-triggered ethernet using colored Petri net. International Conference on Industrial Engineering, Applications and Manufacturing (IKIEAM). 2017; 1-5.
21. Kornienko B. Y. Design and research of mathematical model for Information security system in computer network / B. Y. Kornienko, L. P. Galata. *Science-Based Technologies.* 2017; 34(2): 114-118.
22. White S. C. Comparison of Security Models: Attack Graphs Versus Petri Nets / S. S. White, S. S. Sarvestany. *Advances in Computers*. 2014; 94:1-24.
23. Zhasiul V. Detection and Modeling of Cyber Attacks in Petri Nets / B. Zhasiul, M. Szpyrka, J. Sliva . *Entropy.* 2014; 16; 12: 6602-6623.

Сведения об авторах:

Мещерякова Татьяна Вячеславовна**,** доктор технических наук, начальник кафедры автоматизированных информационных систем органов внутренних дел; tmeshcheriakova4@mvd.ru

Рогозин Евгений Алексеевич, доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел; evgenirogozin@yandex.ru

Ефимов Алексей Олегович, адъюнкт; APMO6@yandex.ru

Романова Виктория Романовна**,** адъюнкт; romanovna_vika@inbox.ru

Коноваленко Сергей Александрович, кандидат технических наук, старший преподаватель кафедры защиты информации специальными методами и средствами; konovalenko_rcf@mail.ru

Information about authors:

Tatyana V. Meshcheryakova, Dr. Sci. (Eng.), Head of the Department of Automated Information Systems of Internal Affairs Bodies; tmeshcheriakova4@mvd.ru

Evgeny A. Rogozin, Dr. Sci. (Eng.), Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; evgenirogozin@yandex.ru

Alexey O. Efimov, adjunct; APMO6@yandex.ru

Victoria R. Romanova, adjunct; romanovna_vika@inbox.ru

Sergey A. Konovalenko, Cand.Sci. (Eng.), Senior Lecturer of the Department of Information Security by Special Methods and Means; konovalenko_rcf@mail.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 29.05.2022.

Одобрена после рецензирования/ Reviced 18.06.2022.

Принята в печать/Accepted for publication 18.06.2022.