Вестник Дагестанского государственного технического университета. Технические науки. Том 47, №1, 2020
Herald of Daghestan State Technical University.Technical Sciences. Vol.47, No.1, 2020
http://vestnik.dgtu.ru/ISSN (Print) 2073-6185 ISSN (On-line) 2542-095X

Для цитирования: *И.Г. Дровникова, Е.С. Овчинникова, В.В.Конобеевских. Анализ типовых сетевых атак на автоматизированные системы органов внутренних дел. Вестник Дагестанского государственного технического университета. Технические науки. 2020; 47 (1): 72-85. DOI:10.21822/2073-6185-2020-47-1-72-85*
For citation: *I.G. Drovnikova, E.S. Ovchinnikova, V.V. Konobeevsky. Analysis of typical network attacks on automated systems of internal affairs departments. Herald of Daghestan State Technical University. Technical Sciences. 2020; 47(1): 72-85. (In Russ.) DOI:10.21822/2073-6185-2020-47-1-72-85*

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 004.056
DOI:10.21822/2073-6185-2020-47-1-72-85

АНАЛИЗ ТИПОВЫХ СЕТЕВЫХ АТАК НА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

И.Г. Дровникова, Е.С. Овчинникова, В.В.Конобеевских
Воронежский институт Министерства внутренних дел России,
394065, г. Воронеж, пр. Патриотов,53, Россия

Резюме: Цель. *Важными тенденциями теории и практики функционирования современных защищенных автоматизированных систем на объектах информатизации органов внутренних дел являются возрастание числа угроз, реализуемых посредством удаленного несанкционированного доступа (сетевых атак) к конфиденциальному информационному ресурсу, а также усложнение реализации механизмов защиты от них. С целью повышения реальной защищенности существующих и перспективных (разрабатываемых) автоматизированных систем на объектах информатизации органов внутренних дел необходимо определить и проанализировать типовые сетевые атаки, направленные на компоненты и программное обеспечение этих систем.* ***Метод.*** *Методом решения данной задачи является всесторонний анализ процесса реализации сетевых атак на автоматизированные системы при их эксплуатации в защищенном исполнении на объектах информатизации органов внутренних дел.* ***Результат.*** *На основе анализа банка данных угроз безопасности информации, разработанного Федеральной службой по техническому и экспортному контролю России, особенностей эксплуатации современных защищенных автоматизированных систем на объектах информатизации органов внутренних дел, результатов опроса экспертов в области защиты информации выделены в соответствии с семью классификационными признаками и охарактеризованы восемь типов наиболее опасных и часто реализуемых в настоящее время сетевых атак на автоматизированные системы органов внутренних дел с учетом их источников, объектов воздействия и возможных последствий реализации.* ***Вывод.*** *Представленные результаты планируется использовать в дальнейших исследованиях для проведения количественной оценки опасности реализации типовых атак и разработки частной модели актуальных атак для конкретной автоматизированной системыс учетом особенностей ее функционирования в защищенном исполнении на объекте информатизации органа внутренних дел.*

Ключевые слова: *защита информации, информационная безопасность, автоматизированная система, информационная угроза, несанкционированный доступ, сетевая атака*

COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

ANALYSIS OF TYPICAL NETWORK ATTACKS ON AUTOMATED SYSTEMS OF INTERNAL AFFAIRS DEPARTMENTS

I.G. Drovnikova, E.S. Ovchinnikova, V.V. Konobeevsky
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov St., Voronezh 394065, Russia

Abstract. Aim *Important contemporary trends in the theory and functional practice of secure automated systems at informatisation facilities of internal affairs bodies include an increase in the number of threats realised through remote unauthorised access (network attacks) on confidential information resources, as well as the increasing complexity of implementing mechanisms aimed at providing protection from such attacks. In order to increase the effectiveness of existing and prospective automated security systems at the informatisation facilities of internal affairs bodies, it is necessary to identify and analyse typical network attacks aimed at components and software comprising these systems.* ***Method.*** *The method for solving this problem consists in a comprehensive analysis of the process of implementing network attacks on automated systems when they are used in secure mode in the informatisation facilities of internal affairs bodies.* ***Results.*** *Based on the analysis of information held in the security threat database developed by the Russian Federal Service for Technical and Export Control (FSTEC), modern features and operations of secure automated systems on the informatisation facilities of bodies of internal affairs and the results of a survey of experts in the field of information protection of allocated in accordance with the classification typology, eight types of dangerous attacks on automated systems of the internal affairs bodies are described taking into account their sources, objects, effects and possible consequences of implementation.* ***Conclusion.*** *The presented results are of use in further studies to conduct a quantitative assessment of the danger of typical attacks and for developing a private model of actual attacks for a specific automated system, taking into account their functional features in secure mode operations at the informatisation facility of the internal affairs body.*

Keywords: *information protection, information security, automated system, information threat, unauthorised access, network attack*

Введение. Основными тенденциями последних лет в сфере информатизации органов внутренних дел (ОВД) являются возрастание числа информационных угроз, реализуемых посредством удаленного несанкционированного доступа (НСД) (сетевых атак), направленных на компоненты и программное обеспечение (ПО) автоматизированных систем (АС), а также усложнение реализации механизмов защиты от них на объектах, эксплуатирующих защищенные АС ОВД [1-5]. Обуславливающие данные тенденции причины можно объединить в два блока [6, 7]:

– увеличение количества обрабатываемой конфиденциальной информации, расширение ее номенклатуры, усложнение технологического цикла обработки и др. влекут за собой усложнение и разнообразие программного и аппаратного обеспечения современных АС на объектах информатизации ОВД, необходимого для удовлетворения возрастающих потребностей правоохранительных органов, что, в свою очередь, приводит к росту числа потенциальных уязвимостей и, следовательно, требует решения задачи защиты информации (ЗИ);

– действующие руководящие документы, нормирующие требования к ЗИ современных АС ОВД, не учитывают некоторые появившиеся виды потенциально опасных сетевых атак и расширяющиеся возможности уже известных видов атак, а также увеличение ассортимента методов противодействия им, что приводит к необходимости доработки имеющихся нормативно-распорядительных документов по ЗИ на объектах информатизации ОВД с учетом требований современной международной и отечественной нормативной документации, регламентирующей разработку и эксплуатацию АС ОВД в защищенном исполнении, а также приказов МВД России.

Постановка задачи. Важной задачей является не только анализ, классификация и систематизация уязвимостей компонентов и ПО современных АС ОВД с точки зрения реализации типовых сетевых атак и создание на этой основе таксономии уязвимостей, но также определение и анализ основных типов сетевых атак с целью оценивания опасности их реализации. Результаты проведенной оценки послужат основой для разработки модели актуальных атак с учетом особенностей функционирования современных защищенных АС на объектах информатизации ОВД и формирования предложений в действующие нормативно-распорядительные документы в соответствии с требованиями современной международной, отечественной и ведомственной нормативной документации, регламентирующей разработку и эксплуатацию АС ОВД в защищенном исполнении [2, 8-16].

Методы исследования. При рассмотрении вопроса функционирования АС в защищенном исполнении на объектах информатизации ОВД из всего множества угроз, связанных с НСД к служебной информации, сетевые атаки имеют определяющее значение [7, 17, 18]. Единым понятием «сетевая атака» может быть объединено все многообразие условий и факторов, способных посредством удаленного взаимодействия с объектом воздействия оказывать негативное влияние на безопасность служебной информации в АС ОВД, в том числе на нарушение таких ее потребительских свойств, как конфиденциальность, целостность или доступность, а также на надежность (эффективность) функционирования как системы защиты информации, так и АС ОВД в целом [19-22].

В соответствии с [18] сетевую (удаленную) атаку на АС ОВД будем рассматривать как действие либо совокупность действий, направленных на реализацию угрозы удаленного доступа (с использованием протоколов сетевого взаимодействия) к технологической информации или информации пользователя в компьютерной сети.

Результаты проведенного в [23] анализа позволили определить процентное соотношение нарушений свойств служебной информации в защищенных АС в результате воздействия сетевых атак, применительно к объекту информатизации ОВД: нарушение конфиденциальности (33 %), нарушение целостности (31 %), нарушение доступности (36 %).

Описание способа реализации сетевой атаки сводят, как правило, к описанию виртуального канала ее реализации [7]. В связи с наличием значительного числа уязвимостей компонентов и ПО в практике эксплуатации современных АС ОВД в защищенном исполнении в большинстве случаев имеет место полнодоступный пучок сингулярных каналов (множественный канал) реализации сетевых атак [24]. Имеющаяся статистическая неопределенность использования нарушителем какого-либо из сингулярных каналов, составляющих множественный канал, в значительной мере обусловливает вероятностный характер реализации сетевой атаки по множественному виртуальному каналу на объектах, эксплуатирующих защищенные АС ОВД. Процесс реализации типовой сетевой атаки на информационный ресурс АС, связанный с персональными данными, подробно описан в [13]. В общем случае он включает в себя последовательное прохождение четырех этапов: сбор информации об объекте атаки; вторжение; реализация деструктивных действий; ликвидация следов атаки.

На основе анализа возможных объектов воздействия угроз, широко представленных в [23], и их связи с банком данных угроз БИ (bdu.fstec.ru), разработанным Федеральной службой по техническому и экспортному контролю (ФСТЭК) России, уязвимостей (с точки зрения реализации сетевых атак) компонентов и ПО АС на объектах информатизации ОВД, определенных по итогам опроса экспертов в области обеспечения информационной безопасности, выделены основные объекты воздействия сетевых атак на АС ОВД [25, 26]: ПО, аппаратно-техническое обеспечение, оператор, каналы передачи данных. Для классификации сетевых атак на защищенную АС ОВД используем систему классификационных признаков, предложенную в [13] для телекоммуникационной сети, подключенной к глобальной сети Internet, включающую семь признаков: характер воздействия; цель воздействия; условие начала атаки; наличие обратной связи с атакуемым объектом; расположение субъекта атаки относительно атакуемого объекта; соотношение количества атакуемых объектов и атакующих субъектов; уровень эталонной модели OSI, на котором реализуется атака.

Обсуждение результатов. Анализ 216 угроз, представленных в настоящее время в банке данных угроз БИ, разработанном ФСТЭК России (bdu.fstec.ru), особенностей эксплуатации современных защищенных АС на объектах информатизации ОВД, результатов опроса экспертов в области ЗИ позволил выделить в соответствии с проведенной классификацией восемь типов наиболее опасных и часто реализуемых в настоящее время сетевых атак на АС ОВД [7, 13, 17]. Сформированный перечень включает в себя следующие основные типы атак: анализ сетевого трафика, сканирование сети, «парольная» атака, подмена доверенного объекта сети, навязывание ложного маршрута, внедрение ложного объекта сети, отказ в обслуживании, удаленный запуск приложений.

Проанализируем сетевые атаки на компоненты и ПО защищенной АС ОВД, относящиеся к выделенным типам, с учетом их источников, объектов воздействия и возможных последствий реализации (причиненного ущерба). Перечень атак на АС ОВД, относящихся к типу «Анализ сетевого трафика», с указанием их шифров представлен на рис.1.

Рис.1. Атаки типа «Анализ сетевого трафика» на АС ОВД
Fig.1. Attacks of the «Network Traffic Analysis» type against automated systems of internal affairs bodies

Сетевая атака «Угроза перехвата вводимой и выводимой на периферийные устройства служебной информации» (УБИ. 115), заключается в возможности осуществления нарушителем НСД к служебной информации, вводимой и выводимой на периферийные устройства, путем перехвата данных, обрабатываемых контроллерами периферийных устройств. Источники атаки: внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом. Объекты воздействия: системное ПО, прикладное ПО, аппаратное обеспечение АС ОВД. Возможное последствие реализации атаки — нарушение конфиденциальности служебной информации.

Сетевая атака «Угроза перехвата данных, передаваемых по вычислительной сети» (УБИ. 116) состоит в возможности осуществления нарушителем НСД к сетевому трафику дискредитируемой вычислительной сети в пассивном (иногда в активном) режиме для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз, оставаясь при реализации данной угрозы невидимым (скрытным) получателем перехватываемых данных. Источник атаки — внешний нарушитель с низким потенциалом. Объекты воздействия: сетевой узел, сетевой трафик. Возможное последствие реализации атаки — нарушение конфиденциальности служебной информации.

Сетевая атака «Угроза перехвата привилегированного потока» (УБИ. 117) заключается в возможности осуществления нарушителем НСД к потоку данных, созданного приложением с дополнительными привилегиями, путем синхронного или асинхронного деструктивного программного воздействия на него. Источники атаки: внутренний нарушитель со средним потенциалом, внешний нарушитель со средним потенциалом. Объекты воздействия: системное ПО, прикладное ПО, сетевое ПО. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение целостности, нарушение доступности служебной информации.

Сетевая атака «Угроза перехвата привилегированного процесса» (УБИ. 118) состоит в возможности для нарушителя приобретения права управления процессом, обладающим высокими привилегиями, с целью выполнения произвольного вредоносного кода с правами дискредитированного процесса. Источники атаки: внутренний нарушитель со средним потенциалом, внешний нарушитель со средним потенциалом. Объекты воздействия: системное ПО, приклад-

ное ПО, сетевое ПО. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение целостности, нарушение доступности служебной информации.

Сетевая атака «Угроза перехвата управления гипервизором» (УБИ. 119) заключается в возможности осуществления нарушителем НСД к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым гипервизором, за счет получения нарушителем права управления гипервизором путем эксплуатации уязвимостей консоли управления гипервизором. Источники атаки: внутренний нарушитель со средним потенциалом, внешний нарушитель со средним потенциалом. Объекты воздействия: системное ПО, гипервизор, консоль управления гипервизором. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение целостности, нарушение доступности служебной информации.

Сетевая атака «Угроза перехвата управления средой виртуализации» (УБИ. 120) заключается в возможности осуществления нарушителем НСД к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым всеми гипервизорами, реализующими среду виртуализации, за счёт получения нарушителем права управления этими гипервизорами путём эксплуатации уязвимостей консоли средства управления виртуальной инфраструктурой. Источники атаки: внутренний нарушитель со средним потенциалом, внешний нарушитель со средним потенциалом. Объекты воздействия: АС ОВД, системное ПО. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение целостности, нарушение доступности служебной информации.

2. Сетевая атака на АС ОВД «Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL» (УБИ. 151), относящаяся к типу «Сканирование сети», заключается в возможности получения нарушителем сведений о текущей конфигурации веб-служб и наличии в ней уязвимостей путем исследования WSDL-интерфейса веб-сервера. Источник атаки — внешний нарушитель с низким потенциалом. Объекты воздействия: сетевое ПО, сетевой узел. Возможное последствие реализации атаки — нарушение конфиденциальности служебной информации.

3. Перечень атак на АС ОВД, относящихся к типу «Парольная» атака», с указанием их шифров представлен на рис. 2.

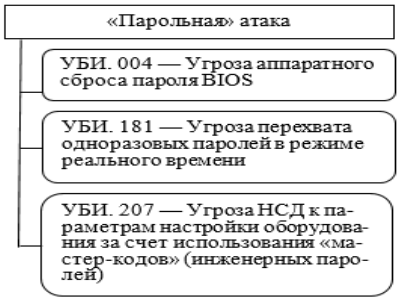

Рис. 2. Атаки типа «Парольная» атака» на АС ОВД
Fig. 2. Attacks of the «Password» attack type on automated systems of internal affairs bodies

Сетевая атака «Угроза аппаратного сброса пароля BIOS» (УБИ. 004) заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путем обесточивания микросхемы BIOS (съема аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»). Источник атаки — внутренний нарушитель, обладающий низким потенциалом. Объекты воздействия: микропрограммное и аппаратное обеспечение BIOS/UEFI. Возможное последствие реализации атаки — нарушение целостности служебной информации.

Сетевая атака «Угроза перехвата одноразовых паролей в режиме реального времени» (УБИ. 181) состоит в возможности для нарушителя получить управление критическими операциями пользователя посредством перехвата одноразовых паролей, которые высылаются системой автома-

тически, для дальнейшего использования их с целью выполнения неправомерных действий прежде, чем истечет их срок действия (обычно не более 5 минут). Источник атаки — внешний нарушитель, обладающий средним потенциалом. Объект воздействия — сетевое ПО. Возможное последствие реализации атаки — нарушение целостности служебной информации.

Сетевая атака «Угроза НСД к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)» (УБИ. 207) состоит в получении несанкционированного доступа к параметрам настройки информации в оборудовании с числовым программным управлением (ЧПУ) путем использования специальных инженерных паролей («мастер-кодов»), «жестко прописанных» в ПО данного оборудования. Источники атаки: внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом. Объекты воздействия: аппаратно-техническое обеспечение, ПО. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение целостности, нарушение доступности служебной информации.

4. Перечень атак на АС ОВД, относящихся к типу «Подмена доверенного объекта сети», с указанием их шифров представлен на рисунке 3.

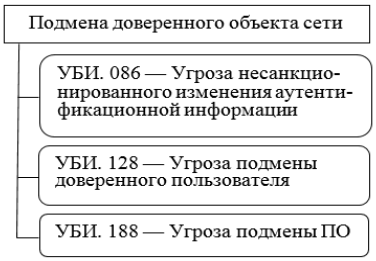

Рис. 3. Атаки типа «Подмена доверенного объекта сети» на АС ОВД
Fig. 3. Attacks of the type «Substitution of a trusted network object» with automated systems of internal affairs bodies

Сетевая атака «Угроза несанкционированного изменения аутентификационной информации» (УБИ. 086) заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств. Источники атаки: внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом. Объекты воздействия: системное ПО, объекты файловой системы, учетные данные пользователя, реестр. Возможные последствия реализации атаки: нарушение целостности, нарушение доступности служебной информации.

Сетевая атака «Угроза подмены доверенного пользователя» (УБИ. 128) заключается в возможности нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно охарактеризовать как «имитация действий клиента». Источник атаки: внешний нарушитель с низким потенциалом. Объекты воздействия: сетевой узел, сетевое ПО. Возможное последствие реализации атаки — нарушение конфиденциальности служебной информации.

Сетевая атака «Угроза подмены ПО» (УБИ. 188) заключается в возможности осуществления нарушителем внедрения в систему вредоносного ПО за счет загрузки и установки вредоносного ПО, скрытого под видом легитимного свободно распространяемого ПО. Источник атаки: внутренний нарушитель со средним потенциалом. Объекты воздействия: прикладное ПО, сетевое ПО, системное ПО. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение целостности, нарушение доступности служебной информации.

5. Перечень атак на АС ОВД, относящихся к типу «Навязывание ложного маршрута», с указанием их шифров представлен на рис. 4.

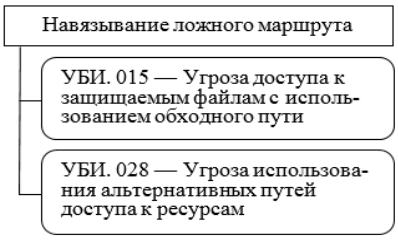

Рис. 4. Атаки типа «Навязывание ложного маршрута» на АС ОВД
Fig. 4. Attacks of the type «Imposing a False Route» on an automated system of internal affairs bodies

Сетевая атака «Угроза доступа к защищаемым файлам с использованием обходного пути» (УБИ. 015) заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему. Источники атаки: внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом. Объекты воздействия — объекты файловой системы. Возможное последствие реализации атаки — нарушение конфиденциальности служебной информации.

Сетевая атака «Угроза использования альтернативных путей доступа к ресурсам» (УБИ. 028) заключается в возможности осуществления нарушителем НСД к защищаемой служебной информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса). Источники атаки: внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом. Объекты воздействия: сетевой узел, объекты файловой системы, прикладное ПО, системное ПО. Возможное последствие реализации атаки — нарушение конфиденциальности служебной информации.

6. Перечень атак на АС ОВД, относящихся к типу «Внедрение ложного объекта сети», с указанием их шифров представлен на рис. 5.

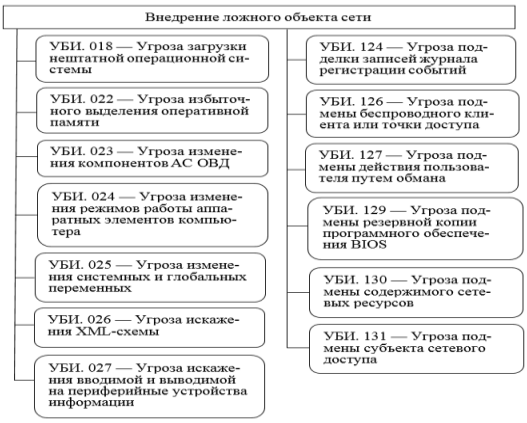

Рис. 5. Атаки типа «Внедрение ложного объекта сети» на АС ОВД
Fig. 5. Attacks of the type "Implementation of a false network object" on an automated system of internal affairs bodies

Сетевая атака «Угроза загрузки нештатной операционной системы» (УБИ.018) заключается в возможности подмены нарушителем загружаемой операционной системы путем несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы. Источник атаки — внутренний нарушитель с низким потенциалом. Объект воздействия — микропрограммное обеспечение BIOS/UEFI. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение целостности, нарушение доступности служебной информации.

Сетевая атака «Угроза избыточного выделения оперативной памяти» (УБИ.022) заключается в возможности выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объема ресурсов оперативной памяти, доступных в АС ОВД для выделения в ответ на запросы программ легальных пользователей. Источники атаки: внутренний нарушитель с низким потенциалом, внешний наруши-

тель с низким потенциалом. Объекты воздействия: аппаратно-техническое обеспечение, системное ПО, сетевое ПО. Возможное последствие реализации атаки — нарушение доступности служебной информации.

Сетевая атака «Угроза изменения компонентов АС ОВД» (УБИ.023) заключается в возможности получения нарушителем доступа к сети, файлам, внедрения закладок и т.д. путем несанкционированного изменения состава программных или аппаратных средств АС ОВД, что в дальнейшем позволит осуществлять данному нарушителю (или другому — внешнему) несанкционированные действия в данной системе. Источник атаки — внутренний нарушитель с низким потенциалом. Объекты воздействия: АС ОВД, сервер, рабочая станция, виртуальная машина, системное ПО, прикладное ПО, аппаратно-техническое обеспечение. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение целостности, нарушение доступности служебной информации.

Сетевая атака «Угроза изменения режимов работы аппаратных элементов компьютер» (УБИ.024) состоит в возможности для нарушителя изменить режимы работы аппаратных элементов компьютера посредством несанкционированного переконфигурирования BIOS/UEFI. Источник угрозы — внутренний нарушитель с высоким потенциалом. Объекты воздействия: микропрограммное и аппаратное обеспечение BIOS/UEFI. Возможные последствия реализации атаки: нарушение целостности, нарушение доступности служебной информации.

Сетевая атака «Угроза изменения системных и глобальных переменных» (УБИ.025) заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на некоторые программы или АС ОВД в целом путем изменения используемых дискредитируемыми программами единых системных и глобальных переменных. Источник атаки — внутренний нарушитель со средним потенциалом. Объекты воздействия: системное ПО, прикладное ПО, сетевое ПО. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение целостности, нарушение доступности служебной информации.

Сетевая атака «Угроза искажения XML-схемы» (УБИ.026) заключается в возможности изменения нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние «отказ в обслуживании», путем изменения XML-схемы, передаваемой между клиентом и сервером. Источники атаки: внутренний нарушитель со средним потенциалом, внешний нарушитель со средним потенциалом. Объекты воздействия: сетевой узел, сетевое ПО, сетевой трафик. Возможные последствия реализации атаки: нарушение целостности, нарушение доступности служебной информации.

Сетевая атака «Угроза искажения вводимой и выводимой на периферийные устройства информации» (УБИ.027) заключается в возможности дезинформирования пользователей или автоматических систем управления путем подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения служебной информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства. Источники атаки: внутренний нарушитель с низким потенциалом, внешний нарушитель с высоким потенциалом. Объекты воздействия: системное ПО, прикладное ПО, сетевое ПО, аппаратно-техническое обеспечение. Возможное последствие реализации атаки — нарушение целостности служебной информации.

Сетевая атака «Угроза подделки записей журнала регистрации событий» (УБИ. 124) заключается в возможности внесения нарушителем изменений в журналы регистрации событий безопасности дискредитируемой системы для введения в заблуждение ее администраторов или сокрытия следов реализации других угроз. Источники атаки: внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом. Объект воздействия — системное ПО. Возможное последствие реализации атаки — нарушение целостности служебной информации.

Сетевая атака «Угроза подмены беспроводного клиента или точки доступа» (УБИ. 126) заключается в возможности получения нарушителем аутентификационной или другой защищаемой информации, передаваемой в ходе автоматического подключения точек беспроводного

доступа или клиентского ПО к доверенным субъектам сетевого взаимодействия, подмененным нарушителем. Источник атаки — внешний нарушитель с низким потенциалом. Объекты воздействия: сетевой узел, сетевое ПО, аппаратно-техническое обеспечение, точка беспроводного доступа. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение доступности служебной информации.

Сетевая атака «Угроза подмены действия пользователя путем обмана» (УБИ. 127) заключается в возможности нарушителя выполнения неправомерных действий в АС ОВД от имени другого пользователя с помощью методов социальной инженерии или технических методов. Источник атаки — внешний нарушитель со средним потенциалом. Объекты воздействия: прикладное ПО, сетевое ПО. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение целостности, нарушение доступности служебной информации.

Сетевая атака «Угроза подмены резервной копии программного обеспечения BIOS» (УБИ. 129) заключается в возможности опосредованного внедрения нарушителем в BIOS/UEFI дискредитируемого компьютера вредоносного кода, путем ожидания или создания необходимости выполнения процедуры восстановления предыдущей версии ПО BIOS/UEFI, предварительно подмененной нарушителем. Источник атаки — внутренний нарушитель с низким потенциалом. Объекты воздействия: микропрограммное и аппаратное обеспечение BIOS/UEFI. Возможное последствие реализации атаки — нарушение целостности служебной информации.

Сетевая атака «Угроза подмены содержимого сетевых ресурсов» (УБИ. 130) заключается в возможности осуществления нарушителем НСД к защищаемым данным пользователей сети или проведения различных мошеннических действий путем скрытной подмены содержимого хранящихся (сайты, веб-страницы) или передаваемых (электронные письма, сетевые пакеты) по сети данных. Источник атаки — внешний нарушитель с низким потенциалом. Объекты воздействия: прикладное ПО, сетевое ПО, сетевой трафик. Возможное последствие реализации атаки — нарушение конфиденциальности служебной информации.

Сетевая атака «Угроза подмены субъекта сетевого доступа» (УБИ. 131) заключается в возможности осуществления нарушителем НСД к защищаемым данным пользователей сети или проведения различных мошеннических действий путем скрытной подмены в отправляемых дискредитируемым пользователем сетевых запросах сведений об отправителе сообщения. Данную угрозу можно охарактеризовать как «имитация действий сервера». Источник атаки — внешний нарушитель со средним потенциалом. Объекты воздействия: прикладное ПО, сетевое ПО, сетевой трафик. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение целостности служебной информации.

7. Перечень атак на АС ОВД, относящихся к типу «Отказ в обслуживании», с указанием их шифров представлен на рис. 6. Сетевая атака «Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных» (УБИ. 105) заключается в возможности отказа хранилищем больших данных в приеме входных данных неизвестного формата от легального пользователя. Источник атаки — внутренний нарушитель с низким потенциалом. Объекты воздействия: хранилище больших данных, метаданные.

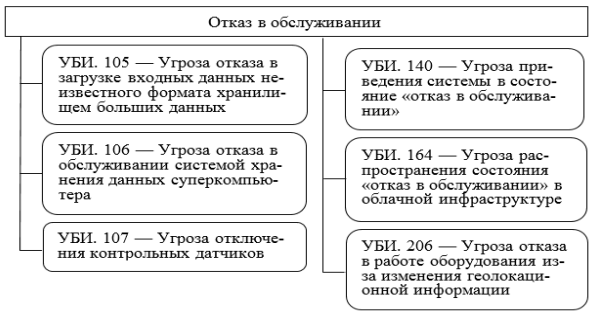

Рис. 6. Атаки типа «Отказ в обслуживании» на АС ОВД
Fig. 6. Denial of service attacks on an automated system of internal affairs bodies

Возможные последствия реализации атаки: нарушение целостности, нарушение доступности служебной информации.

Сетевая атака «Угроза отказа в обслуживании системой хранения данных суперкомпьютера» (УБИ.106) заключается в возможности значительного замедления работы терминальных сессий всех пользователей суперкомпьютера, вплоть до достижения всем суперкомпьютером состояния «отказ в обслуживании» при превышении максимально достижимой нагрузки на параллельную файловую систему суперкомпьютера. Источник атаки - внутренний нарушитель с низким потенциалом. Объект воздействия — система хранения данных суперкомпьютера. Возможное последствие реализации атаки — нарушение доступности служебной информации.

Сетевая атака «Угроза отключения контрольных датчиков» (УБИ.107) заключается в возможности обеспечения нарушителем информационной изоляции системы безопасности путем прерывания канала связи с контрольными датчиками, следящими за параметрами состояния системы, или нарушения работы самих датчиков. Источники атаки: внутренний нарушитель с низким потенциалом, внешний нарушитель с высоким потенциалом. Объект воздействия — системное ПО. Возможные последствия реализации атаки: нарушение целостности, нарушение доступности служебной информации.

Сетевая атака «Угроза приведения системы в состояние «отказ в обслуживании»» (УБИ.140) состоит в возможности для дискредитированной АС ОВД отказать в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой или при использовании недостатков реализации сетевых протоколов. Источники атаки: внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом. Объекты воздействия: АС ОВД, сетевой узел, системное ПО, сетевое ПО, сетевой трафик, телекоммуникационное устройство. Возможное последствие реализации атаки — нарушение доступности служебной информации.

Сетевая атака «Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре» (УБИ. 164) состоит в возможности распространять негативные последствия от реализации угроз на физическом или виртуальном уровне как на другие уровни (управления и оркестровки) облачной инфраструктуры, так и на все АС, которые развернуты на объектах информатизации ОВД на основе дискредитированной облачной инфраструктуры. Источники атаки: внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом. Объекты воздействия: облачная инфраструктура, созданная с использованием технологий виртуализации. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение целостности, нарушение доступности служебной информации.

Сетевая атака «Угроза отказа в работе оборудования из-за изменения геолокационной информации» (УБИ.206) состоит в прекращении работы оборудования с ЧПУ за счет изменения геолокационной информации о данном оборудовании. Источник атаки — внешний нарушитель с высоким потенциалом, Объект воздействия — аппаратно-техническое устройство. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение доступности служебной информации.

8. Перечень атак на АС ОВД, относящихся к типу «Удаленный запуск приложений», с указанием их шифров представлен на рис. 7. Сетевая атака «Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы» (УБИ.195) заключается в возможности удаленного запуска вредоносного кода за счет создания приложений, использующих обход встроенных в операционную систему механизмов защиты. Источник атаки — внешний нарушитель с высоким потенциалом. Объекты воздействия: стационарные и мобильные устройства (компьютеры и ноутбуки) (аппаратное устройство).

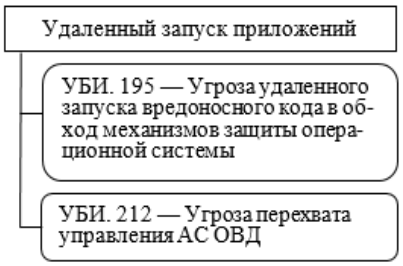

Рис. 7. Атаки типа «Удаленный запуск приложений» на АС ОВД
Fig. 7. Attacks of the «Remote Application Launch» type against an automated system of internal affairs bodies

Возможное последствие реализации атаки — нарушение целостности служебной информации. Сетевая атака «Угроза перехвата управления АС ОВД» (УБИ.212) заключается в возможности осуществления нарушителем НСД к информационным, программным и вычислительным ресурсам АС ОВД в результате подмены средств централизованного управления системой или ее компонентами. Источник атаки — внутренний нарушитель со средним потенциалом. Объект воздействия — инфраструктура АС ОВД. Возможные последствия реализации атаки: нарушение конфиденциальности, нарушение целостности, нарушение доступности служебной информации.

Вывод. В статье сформирован перечень основных сетевых атак на АС ОВД, включающий восемь типов наиболее опасных и часто реализуемых в настоящее время атак, классифицированных по семи признакам. Представлено описание выделенных типов атак с учетом их источников, объектов воздействия и возможных последствий реализации (причиненного ущерба).

Результаты анализа сетевых атак из сформированного перечня, позволят провести количественную оценку опасности их реализации, что послужит основой для разработки частной модели актуальных атак для конкретной АС с учетом особенностей ее функционирования в защищенном исполнении на объекте информатизации ОВД. Это позволит сформировать предложения в действующие нормативно-распорядительные документы по ЗИ в АС ОВД в соответствии с требованиями современной международной, отечественной и ведомственной нормативной документации, регламентирующей разработку и эксплуатацию АС ОВД в защищенном исполнении, с целью повышения реальной защищенности существующих и перспективных (разрабатываемых) АС на объектах информатизации ОВД.

Библиографический список:

1. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646 [Электронный ресурс]. — URL:http://publication.pravo.gov.ru/Document/ View/0001201612060002 (дата обращения: 14.11.2019).
2. Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года: приказ МВД России от 14.03.2012 № 169 [Электронный ресурс]. RL:http://policemagazine.ru/forum/showthread. php?t=3663 (дата обращения: 27.11.2019).
3. Butusov I.V. Methodology of Security Assessment Automated Systems as Objects Critical Information Infrastructure / I.V. Butusov, A.A. Romanov [Электронный ресурс]. — URL:fcyberrus.com/wp-content/uploads/ 2018/05/02-10-125-18_1.-Butusov.pd (дата обращения: 28.11.2019).
4. Maximizing Uptime of Critical Systems in Commercial and Industrial Applications VAVR-8K4TVA_R1_EN.pdf [Электронный ресурс]. — URL:https://download.schneider-eletric. com/files?p_Doc_Ref=SPD_VAVR-8K4TVA_EN (дата обращения: 04.12.2019).
5. Xin Z. Research on effectiveness evaluation of the mission-critical system / Z. Xin, M. Shaojie, Z. Fang // Proceedings of 2013 2nd International Conference on Measurement, Information and Control. 2013. pp. 869-873.
6. Методы и средства эволюционного и структурного моделирования при обосновании требований к программным системам защиты информации: монография / Змеев А.А. [и др.]; под ред. Е.А. Рогозина. — Воронеж: Воронежский институт МВД России, 2015. — 92 с.
7. Язов Ю.К. Защита информации в информационных системах от несанкционированного доступа / Ю.К. Язов, С.В. Соловьев. — Воронеж: Кварта, 2015. — 440 с.
8. 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 18.11.2019).
9. ГОСТ Р 51583-2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении [Электронный ресурс]. URL:http://docs.cntd.ru/document/1200108858 (дата обращения: 21.11.2019).
10. 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/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (дата обращения 24.11.2019).

11. 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: 18.11.2019).
12. ФСТЭК РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [Электронный ресурс]. — URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g (дата обращения: 24.11.2019).
13. ФСТЭК России. Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка), 2008 год [Электронный ресурс]. URL:https://fstec.ru/component/attachments/ download/289 (дата обращения: 24.11.2019).
14. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения [Электронный ресурс]. URL:http://docs.cntd.ru/document/1200058320 (дата обращения: 27.11.2019).
15. Руководящий документ Государственной технической комиссии 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: 13.12.2019).
16. 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: 24.11.2019).
17. Радько Н.М. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа / Н.М. Радько, Ю.К. Язов, Н.Н. Корнеева. Воронеж: Воронеж. госуд. технич. ун-т, 2013. 265 с.
18. Язов Ю.К. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. Воронеж: Кварта, 2018. 588 с.
19. Kresimir S. The information systems' security level assessment model based on an ontology and evidential reasoning approach / S. Kresimir, O. Hrvoje, G. Marin // Computers & Security. 2015. pp. 100-112.
20. 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.
21. Method to Evaluate Software Protection Based on Attack Modeling / H. Wang [et ol.] // 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing Year. 2013. pp. 837-844.
22. Effectiveness Evaluation on Cyberspace Security Defense System / L. Yun [et ol.] // International Conference on Network and Information Systems for Computers (IEEE Conference Publications). 2015. pp. 576-579.
23. Применение новых информационных технологий при разработке тренажерных комплексов в интересах Вооруженных сил Российской федерации: монография / Махинов Д.В. [и др.] — Воронеж: ВУНЦ ВВС «ВВА» им. профессора Н.Е. Жуковского и Ю.А. Гагарина, 2016. 200 с.
24. Методы и средства оценки защищенности автоматизированных систем органов внутренних дел: монография [Электронный ресурс] / Дровникова И.Г. [и др.]. Воронеж: Воронеж. ин-т МВД России, 2017. 88 с.
25. Попов А.Д. Модели и алгоритмы оценки эффективности систем защиты информации от несанкционированного доступа с учетом их временных характеристик в автоматизированных системах органов внутренних дел: дис. ... канд. техн. наук: 05.13.19 / Попов Антон Дмитриевич. Воронеж, 2018. 163 с.
26. Попов А.Д. Классификация угроз информационной безопасности в автоматизированных информационных системах / Е.А. Рогозин, А.Д. Попов, Д.И. Коробкин // Приборы и системы. Управление, контроль, диагностика. — 2017. № 7. С. 22–26.

References:

1. Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii: ukaz Prezidenta RF ot 05.12.2016 № 646 [Elektronnyy resurs]. — URL:http://publication.pravo.gov.ru/Document/ View/0001201612060002 (data obrashcheniya: 14.11.2019). [On approval of the Doctrine of Information Security of the Russian Federation: Decree of the President of the Russian Federation dated December 05, 2016 No. 646 [Electronic resource]. - URL: http: //publication.pravo.gov.ru/Document/ View / 0001201612060002 (accessed: 11/14/2019). (In Russ.)]
2. Ob utverzhdenii Kontseptsii obespecheniya informatsionnoy bezopasnosti organov vnutrennikh del Rossiyskoy Federatsii do 2020 goda: prikaz MVD Rossii ot 14.03.2012 № 169 [Elektronnyy resurs]. RL:http://policemagazine.ru/forum/showthread. php?t=3663 (data obrashcheniya: 27.11.2019) [On approval of the Concept of ensuring information security of the internal affairs bodies of the Russian Federation until 2020: Order of the Ministry of Internal Affairs of Russia dated 14.03.2012 No. 169 [Electronic resource]. RL: http: //policemagazine.ru/forum/showthread. php? t = 3663 (accessed: 11/27/2019) (In Russ.)]
3. Butusov I.V. Methodology of Security Assessment Automated Systems as Objects Critical Information Infrastructure / I.V. Butusov, A.A. Romanov [Electronic resource]. - URL: fcyberrus.com/wp-content/uploads/ 2018/05 / 02-10-125-18_1. Butusov.pd (accessed: 11.28.2019).
4. Maximizing Uptime of Critical Systems in Commercial and Industrial Applications VAVR-8K4TVA_R1_EN.pdf [Electronic resource]. - URL: https: //download.schneider-eletric. com / files? p_Doc_Ref = SPD_VAVR-8K4TVA_EN (Date accessed: 12/04/2019).
5. Xin Z. Research on effectiveness evaluation of the mission-critical system / Z. Xin, M. Shaojie, Z. Fang // Proceedings of 2013 2nd International Conference on Measurement, Information and Control. 2013 . pp. 869-873(In Russ.)]
6. Metody i sredstva evolyutsionnogo i strukturnogo modelirovaniya pri obosnovanii trebovaniy k programmnym sistemam zashchity informatsii: monografiya / Zmeyev A.A. [i dr.]; pod red. Ye.A. Rogozina. — Voronezh: Voronezhskiy institut MVD Rossii, 2015. 92 s. [Methods and tools of evolutionary and structural modeling when substantiating requirements for software information protection systems: monograph / Zmeev A.A. [and etc.]; under the editorship of E.A. Rogozin. - Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia, 2015. 92 p. (In Russ.)]

7. YAzov YU.K. Zashchita informatsii v informatsionnykh sistemakh ot nesanktsionirovannogo dostupa / YU.K. YAzov, S.V. Solov'yev. Voronezh: Kvarta, 2015. 440 s [Yazov Yu.K. Information security in information systems from unauthorized access / Yu.K. Yazov, S.V. Soloviev. - Voronezh: Quarta, 2015. 440 p. (In Russ.)]
8. GOSTR ISO/MEK 15408-2-2013. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. CH. 2: Funktsional'nyye komponenty bezopasnosti [Elektronnyy resurs]. — URL:http://docs.cntd. ru/document/1200105710 (data obrashcheniya 18.11.2019). [GOSTR ISO / IEC 15408-2-2013. Information technology. Security methods and tools. Criteria for assessing the security of information technology. Part 2: Functional components of security [Electronic resource]. - URL: http: //docs.cntd. com / document / 1200105710 (accessed 11/18/2019) (In Russ.)]
9. . GOST R 51583-2014. Natsional'nyy standart Rossiyskoy Federatsii. Zashchita informatsii. Poryadok sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii [Elektronnyy resurs]. URL:http://docs.cntd.ru/document/1200108858 (data obrashcheniya: 21.11.2019). [GOST R 51583-2014. National standard of the Russian Federation. Protection of information. The procedure for creating automated systems in a protected version [Electronic resource]. URL: http: //docs.cntd.ru/document/1200108858 (accessed date: 11/21/2019) (In Russ.)]
10. . FSTEK RF. Rukovodyashchiy dokument. Avtomatizirovannyye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii [Elektronnyy resurs]. — URL:https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (data obrashcheniya 24.11.2019). [FSTEC of the Russian Federation. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and information protection requirements [Electronic resource]. - URL: https: //fstec.ru/ tekhnicheskaya-zashchita-informatsii / dokumenty / 114-spetsialnye-normativnye-dokumenty / 384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-mart (date of treatment 11.24.2019) (In Russ.)]
11. FSTEK RF. Rukovodyashchiy dokument. Kontseptsiya zashchity sredstv vychislitel'noy tekhniki i avtomatizirovannykh sistem ot nesanktsionirovannogo dostupa k informatsii.[Elektronnyy resurs]. URL:http://fstec.ru/component/attachments/download/299 (data obrashcheniya: 18.11.2019). [FSTEC of the Russian Federation. Guidance document. The concept of protecting computer equipment and automated systems from unauthorized access to information. [Electronic resource]. URL: http: //fstec.ru/component/attachments/download/299 (accessed: 11/18/2019) (In Russ.)]
12. FSTEK RF. Rukovodyashchiy dokument. Sredstva vychislitel'noy tekhniki. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Pokazateli zashchishchennosti ot nesanktsionirovannogo dostupa k informatsii [Elektronnyy resurs]. — URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g (data obrashcheniya: 24.11.2019). FSTEC of the Russian Federation. Guidance document. Computer facilities. Protection against unauthorized access to information. Indicators of security against unauthorized access to information [Electronic resource]. - URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyuly (Date of treatment: 11.24.2019) (In Russ.)]
13. FSTEK Rossii. Metodicheskiy dokument. Bazovaya model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh (vypiska), 2008 god [Elektronnyy resurs]. URL:https://fstec.ru/component/attachments/ download/289 (data obrashcheniya: 24.11.2019). [FSTEC of Russia. Methodical document. The basic model of personal data security threats during their processing in personal data information systems (extract), 2008 [Electronic resource]. URL: https: //fstec.ru/component/attachments/ download / 289 (accessed: 11.24.2019 (In Russ.)]
14. GOST R 50922-2006. Zashchita informatsii. Osnovnyye terminy i opredeleniya [Elektronnyy resurs]. URL:http://docs.cntd.ru/ document/1200058320 (data obrashcheniya: 27.11.2019). [GOST R 50922-2006. Protection of information. Basic terms and definitions [Electronic resource]. URL: http: //docs.cntd.ru/ document / 1200058320 (accessed: 11/27/2019) (In Russ.)]
15. Rukovodyashchiy dokument Gosudarstvennoy tekhnicheskoy komissii ot 30 iyunya 1992 goda. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Terminy i opredeleniya. [Elektronnyy resurs]. URL: https://fstec.ru/component/attachments/download/298 (data obrashcheniya: 13.12.2019). [Guidance document of the State Technical Commission of June 30, 1992. Protection against unauthorized access to information. Terms and Definitions. [Electronic resource]. URL: https://fstec.ru/component/attachments/download/298 (accessed: 12/13/2019) (In Russ.)]
16. Rukovodyashchiy dokument Gosudarstvennoy tekhnicheskoy komissii pri Prezidente Rossiyskoy Federatsii ot 30 marta 1992 goda. Avtomatizirovannyye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii [Elektronnyy resurs]. — URL:http://files.stroyinf.ru/Data2/1/4293809/4293809157.htm (data obrashcheniya: 24.11.2019). [The governing document of the State Technical Commission under the President of the Russian Federation of March 30, 1992. Automated systems. Protection against unauthorized access to information. Classification of automated systems and information protection requirements [Electronic resource]. - URL: http: //files.stroyinf.ru/Data2/1/4293809/4293809157.htm (accessed: 11.24.2019) (In Russ.)]
17. Rad'ko N.M. Proniknoveniya v operatsionnuyu sredu komp'yutera: modeli zloumyshlennogo udalennogo dostupa / N.M. Rad'ko, YU.K. YAzov, N.N. Korneyeva. — Voronezh: Voronezh. gosud. tekhnich. un-t, 2013. — 265 s. [Radko N.M. Penetration into the computer's operating environment: malicious remote access models / N.M. Radko, Yu.K. Yazov, N.N. Korneeva. - Voronezh: Voronezh. gos. tech. Univ., 2013. 265 p. (In Russ.)]
18. YAzov YU.K. Organizatsiya zashchity informatsii v informatsionnykh sistemakh ot nesanktsionirovannogo dostupa: monografiya / YU.K. YAzov, S.V. Solov'yev. — Voronezh: Kvarta, 2018. — 588 s. [Yazov Yu.K. Organization of information protection in information systems from unauthorized access: monograph / Yu.K. Yazov, S.V. Soloviev. Voronezh: Quart, 2018. 588 p. (In Russ.)]
19. Kresimir S. The information systems' security level assessment model based on an ontology and evidential reasoning approach / S. Kresimir, O. Hrvoje, G. Marin // Computers & Security. — 2015. — P. 100-112.
20. 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.
21. Method to Evaluate Software Protection Based on Attack Modeling / H. Wang [et ol.] // 2013 IEEE 10th International Conference on

High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing Year. 2013. pp. 837-844.

22. Effectiveness Evaluation on Cyberspace Security Defense System / L. Yun [et ol.] // International Conference on Network and Information Systems for Computers (IEEE Conference Publications). 2015. pp. 576-579. 23.
23. Primeneniye novykh informatsionnykh tekhnologiy pri razrabotke trenazhernykh kompleksov v interesakh Vooruzhen-nykh sil Rossiyskoy Federatsii: monografiya / Makhinov D.V. [i dr.] — Voronezh: VUNTS VVS «VVA» im. professora N.Ye. Zhukovskogo i YU.A. Gagarina, 2016. 200 s. [The use of new information technologies in the development of training complexes in the interests of the Armed forces of the Russian Federation: monograph / Makhinov DV [and others] - Voronezh: VUNC Air Force "VVA" them. professors N.E. Zhukovsky and Yu.A. Gagarina, 2016.200 s. (In Russ.)]
24. Metody i sredstva otsenki zashchishchennosti avtomatizirovannykh sistem organov vnutrennikh del: monografiya [Elektronnyy resurs] / Drovnikova I.G. [i dr.]. Voronezh: Voronezh. in-t MVD Rossii, 2017. 88 s. [Methods and means of assessing the security of automated systems of internal affairs bodies: monograph [Electronic resource] / Drovnikova I.G. [and etc.]. Voronezh: Voronezh. Institute of the Ministry of Internal Affairs of Russia, 2017. 88 p. (In Russ.)]
25. Popov A.D. Modeli i algoritmy otsenki effektivnosti sistem zashchity informatsii ot nesanktsionirovannogo dostupa s uchetom ikh vremennykh kharakteristik v avtomatizirovannykh sistemakh organov vnutrennikh del: dis. ... kand. tekhn. nauk: 05.13.19 / Popov Anton Dmitriyevich. Voronezh, 2018. 163 s. [Popov A.D. Models and algorithms for evaluating the effectiveness of information protection systems against unauthorized access, taking into account their time characteristics in automated systems of internal affairs bodies: dis. ... cand. tech. Sciences: 05.13.19 / Popov Anton Dmitrievich. Voronezh, 2018.163 p. (In Russ.)]
26. Popov A.D. Klassifikatsiya ugroz informatsionnoy bezopasnosti v avtomatizirovannykh informatsionnykh sistemakh / Ye.A. Rogozin, A.D. Popov, D.I. Korobkin // Pribory i sistemy. Upravleniye, kontrol', diagnostika. — 2017. № 7. S. 22–26. [Popov A.D. Classification of threats to information security in automated information systems / E.A. Rogozin, A.D. Popov, D.I. Korobkin // Devices and systems. Management, control, diagnostics. 2017. No. 7. pp. 22–26. (In Russ.)]

Сведения об авторах:

Дровникова Ирина Григорьевна, доктор технических наук, доцент, профессор кафедры автоматизированных информационных систем органов внутренних дел; e-mail.ru: idrovnikova@mail.ru

Конобеевских Владимир Валерьевич**,** кандидат технических наук, доцент кафедры автоматизированных информационных систем органов внутренних дел; e-mail.ru: vkonobeevskikh@mail.ru

Овчинникова Елена Сергеевна**,** адъюнкт кафедры автоматизированных информационных систем органов внутренних дел; e-mail.ru:yelena_ovchinnikova1@mail.ru

Information about authors:

Irina G. Drovnikova, Dr. Sci. (Technical), Assoc. Prof., Prof., Department of Automated Information Systems of the Internal Affairs Bodies; e-mail.ru: idrovnikova@mail.ru

Vladimir V.Konobeyevskikh, Cand. Dr. Sci.(Technical), Assoc. Prof., Department of Automated Information Systems of the Internal Affairs Bodies; e-mail.ru: vkonobeevskikh@mail.ru

Elena S. Ovchinnikova, Adjunct, Department of Automated Information Systems of the Internal Affairs Bodies; e-mail.ru:yelena_ovchinnikova1@mail.ru

Конфликт интересов.

Авторы заявляют об отсутствии конфликта интересов.

Поступила в редакцию 15.01.2020.

Принята в печать 19.02.2020.

Conflict of interest.

The authors declare no conflict of interest.

Received 15.01. 2020.

Accepted for publication 19.02.2020.