Анна В. Бацких[1], Ирина Г. Дровникова[2], Елена С. Овчинникова[3], Евгений А. Рогозин[4]
[1,2,3,4]Воронежский институт министерства внутренних дел Российской федерации, пр-т Патриотов, 53, Воронеж, 394065, Россия
[1]e-mail: svatikova96@mail.ru, https://orcid.org/0000-0001-5564-168X
[2]e-mail: idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875
[3]e-mail: yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524
[4]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

АНАЛИЗ И КЛАССИФИКАЦИЯ ОСНОВНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

DOI: http://dx.doi.org/10.26583/bit.2020.1.04

Аннотация. В статье представлены результаты анализа угроз, реализуемых посредством удаленного несанкционированного доступа (НСД) (сетевых атак) к информационному ресурсу автоматизированных систем (АС) на объектах информатизации органов внутренних дел (ОВД), представленных на официальном сайте федеральной службы по техническому и экспортному контролю (ФСТЭК) России (bdu.fstec.ru). На основе анализа международных и отраслевых стандартов Российской Федерации, нормативно-методической документации ФСТЭК России, ведомственной документации МВД России, нормирующих требования по информационной безопасности (ИБ), научно-технической литературы в области защиты информации (ЗИ) разработаны трехуровневая иерархия и классификационная схема угроз, связанных с НСД к информационному ресурсу АС ОВД. Анализ банка данных угроз безопасности информации, разработанного ФСТЭК России, уязвимостей компонентов и программного обеспечения (ПО) АС на объектах информатизации ОВД с точки зрения реализации сетевых атак, определенных по итогам опроса экспертов в области обеспечения ИБ, позволил раскрыть содержание этапов типовой сетевой атаки и провести классификацию атак на АС ОВД, используя семь классификационных признаков. В соответствии с проведенной классификацией разработан перечень основных атак на АС ОВД, включающий восемь типов наиболее опасных и часто реализуемых в настоящее время сетевых атак с учетом возможных последствий их реализации. Представленные результаты планируется использовать в дальнейших исследованиях для проведения количественной оценки опасности реализации выделенных атак и 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 с целью повышения реальной защищенности существующих и перспективных (разрабатываемых) АС на объектах информатизации ОВД.

Ключевые слова: защита информации, информационная безопасность, автоматизированная система, несанкционированный доступ, уязвимость, информационная угроза, сетевая атака.
Для цитирования: БАЦКИХ, Анна В. et al. АНАЛИЗ И КЛАССИФИКАЦИЯ ОСНОВНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ. Безопасность информационных технологий, [S.l.], v. 27, n. 1, p. 40-50, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1250>. Дата доступа: 10 feb. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.1.04.

Anna V. Batskih[1], Irina G. Drovnikova[2], Elena S. Ovchinnikova[3], Evgeni A. Rogozin[4]
[1,2,3,4]Voronezh Institute of the Ministry of the Interior, Prospect Patriotov, 53, Voronezh, 394065, Russia
[1]e-mail: svatikova96@mail.ru, https://orcid.org/0000-0001-5564-168X
[2]e-mail: idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875
[3]e-mail: yelena_ovchinnikova1@mail.ru, https://orcid.org/0000-0003-4139-9524
[4]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

Analysis and classification of the main threats to information security of automated systems at the objects of informatization of internal affairs bodies

DOI: http://dx.doi.org/10.26583/bit.2020.1.04

Abstract. The paper presents the results of the analysis of threats implemented through remote unauthorized access (UA) (network attacks) to the information resource of automated systems (AS) at the objects of Informatization of internal Affairs bodies (ATS), presented on the official website of the Federal service for technical and export control (FSTEC) of Russia (bdu.fstec.ru). Based on the analysis of international and sectoral standards of the Russian Federation, as well as regulatory documents of the FSTEC of Russia, and departmental documentation of the MIA of Russia, and the fiducial requirements on information security (IS), and scientific literature in the field of information protection (IP) it is developed a three-tiered hierarchy and classification scheme of the threats related to unauthorized access to the information resource as ATS. The analysis of the data Bank of information security threats developed by FSTEC of Russia, as well as vulnerabilities of components and software (SW) of ATS at ATS Informatization objects in terms of implementation of network attacks determined by the results of a survey of experts in the field of information security, allowed to reveal the content of the stages of a typical network attack and to classify attacks on ATS, using seven classification criteria. In accordance with the classification it was developed a list of the main attacks on ATS, including eight types of the most dangerous and often implemented at the present time network attacks, also taking into account the possible consequences of their implementation. The presented results are planned to be used in further quantitative assessment of the danger of the implementation of selected attacks and to develop a private model of actual attacks for a specific AU, taking into account the peculiarities of its functioning in a protected version at the ATS Informatization facility. This will allow making a number or proposals for the existing regulatory and administrative documents on IP in ATS in order to increase the real security of existing and prospective (developed) ACS at ATS Informatization facilities.

Keywords: information protection, information security, automated system, unauthorized access, vulnerability, information threat, network attack.

For citation: BATSKIH, Anna V. et al. Analysis and classification of the main threats to information security of automated systems at the objects of informatization of internal affairs bodies. IT Security (Russia), [S.l.], v. 27, n. 1, p. 40-50, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1250>. Date accessed: 10 feb. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.1.04.

Введение

Настоящее время характеризуется широким внедрением новых информационных технологий (ИТ) на объектах информатизации специального назначения, в том числе на объектах, эксплуатирующих защищенные АС ОВД, предназначенные для обработки, хранения и передачи конфиденциальной информации. При этом практика использования ИТ при эксплуатации АС ОВД в защищенном исполнении без увязки с обеспечением их ИБ существенно повышает вероятность проявления информационных угроз [1].

Постоянная модернизация АС ОВД ведет к значительному усложнению проблемы, связанной с защитой их информационного ресурса. Это обуславливается рядом внутренних противоречий, определяемых современными тенденциями развития ИТ [2]:

– между усложнением разнообразного программного и аппаратного обеспечения современных АС на объектах информатизации ОВД, необходимого для удовлетворения растущих потребностей правоохранительных органов (увеличение количества обрабатываемой конфиденциальной информации, расширение ее номенклатуры, усложнение технологического цикла обработки и др.), с одной стороны, и необходимостью решения задачи защиты конфиденциальной информации – с другой. В свою очередь, усложнение разнообразного программного и аппаратного обеспечения современных АС ОВД приводит к увеличению числа потенциальных уязвимостей;

– между широким ассортиментом и возрастающими возможностями реализации

разновидностей угроз безопасности информации в реально функционирующих АС ОВД, с одной стороны, и необходимостью не только разработки руководящей документации по ЗИ на объектах информатизации ОВД, включающей модели неизвестных видов угроз, но и постоянного пересмотра существующих моделей уже известных видов угроз, а также разработки требований по ЗИ – с другой. В настоящее время ЗИ на объектах информатизации ОВД, осуществляемая в соответствии с требованиями действующей нормативно-распорядительной документации, не учитывает некоторые появившиеся виды потенциально опасных угроз безопасности информации в АС ОВД или расширяющиеся возможности уже известных видов угроз. В то же время неуклонный рост номенклатуры угроз безопасности информации в АС ОВД и методов противодействия им 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.

1. Постановка задачи

На основе вышеизложенного важной задачей является не только анализ, классификация и систематизация уязвимостей компонентов и ПО современных АС ОВД с точки зрения реализации основных угроз безопасности информации и создание на этой основе таксономии уязвимостей, но и анализ, классификация основных угроз с целью оценивания опасности их реализации. Результаты проведенной оценки послужат основой для разработки модели актуальных угроз с учетом особенностей функционирования современных АС в защищенном исполнении 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. Теоретический анализ

Все многообразие факторов и условий, способных оказывать непосредственное негативное влияние на безопасность информации в АС, в том числе на нарушение таких ее потребительских свойств, как конфиденциальность, целостность или доступность, а также на надежность (эффективность) функционирования как системы защиты информации (СЗИ) АС ОВД, так и системы в целом, может быть объединено единым понятием «угроза безопасности информации». В [3, 4] угроза безопасности информации в АС трактуется как совокупность факторов и условий, создающих потенциально существующую либо реальную опасность утечки, хищения, утраты, уничтожения, искажения, модификации, подделки, копирования, блокирования информации и НСД к ней. Из всего многообразия угроз безопасности информации по способу их реализации в АС ОВД особо выделяются угрозы, связанные с НСД. В соответствии с [5] под НСД понимается доступ к конфиденциальной информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС. К угрозам, связанным с НСД к информационному ресурсу защищенных АС ОВД, следует отнести: несанкционированное ознакомление, несанкционированное копирование (хищение) и/или несанкционированное воздействие на служебную информацию (блокирование, уничтожение и т.д.) [6].

В общем случае описание угрозы безопасности информации представляет собой кортеж из 7 элементов (рис. 1) [6], отдельные элементы которого могут либо

отсутствовать, либо также рассматриваться как кортежи со сложной структурой. При необходимости описание некоторых угроз может быть расширено добавлением новых элементов.

$$U = \langle \text{<наименование угрозы>, <источник угрозы>, <реализуемая уязвимость (совокупность уязвимостей)>, <способ реализации угрозы>, <несанкционированное действие, выполняемое при реализации угрозы>, <время существования угрозы>, <время, необходимое на реализацию угрозы>} \rangle$$

Рис. 1. Структура кортежа описания угрозы безопасности информации в АС ОВД (Fig. 1. The structure of the tuple description of information security threats in ATS)

Угроза, как правило, именуется по наименованию несанкционированного действия.

Согласно [7] источник угрозы безопасности информации представляет собой субъект доступа, материальный объект или физическое явление, служащее причиной возникновения угрозы, а несанкционированное действие – действие с информацией, осуществляемое с нарушением установленных прав и/или правил действий с ней с применением штатных средств АС или средств, аналогичных им по функциональному предназначению и техническим характеристикам.

Описание способа реализации угрозы сводят, как правило, к описанию канала ее реализации (канала НСД или канала несанкционированного воздействия) [6].

Виртуальный канал НСД к информации включает в себя субъекта доступа, а также путь доступа в операционную среду компьютера и к блоку защищаемой информации. В связи с наличием значительного числа уязвимостей ПО в практике эксплуатации АС ОВД в защищенном исполнении в большинстве случаев имеет место полнодоступный пучок сингулярных каналов реализации угроз (то есть существуют множественные каналы, характеризующиеся возможностью использования нескольких путей к защищаемому блоку информации, но неизвестно, который из них выберет нарушитель для реализации угрозы) [8]. Имеющаяся статистическая неопределенность использования какого-либо из сингулярных каналов, составляющих множественный канал, в значительной мере обусловливает вероятностный характер реализации угрозы по множественному виртуальному каналу.

3. Анализ результатов

С учетом выше изложенного на основе анализа международных и отраслевых стандартов Российской Федерации по ИБ АС [4, 9, 10], нормативно-методической документации ФСТЭК России, посвященной разработке базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных [7], ведомственной документации МВД России, регламентирующей требования по ЗИ на объектах информатизации ОВД [3], научно-технической литературы в области обеспечения ИБ [6, 11, 12, 14] разработана иерархия угроз НСД, направленных на нарушение ИБ АС ОВД (рис. 2).

В представленной иерархии можно выделить три уровня угроз:

1-й уровень – угрозы, направленные на получение доступа к элементам АС ОВД;

2-й уровень – угрозы доступа к обрабатываемой конфиденциальной информации;

3-й уровень – угрозы выполнения несанкционированных действий.

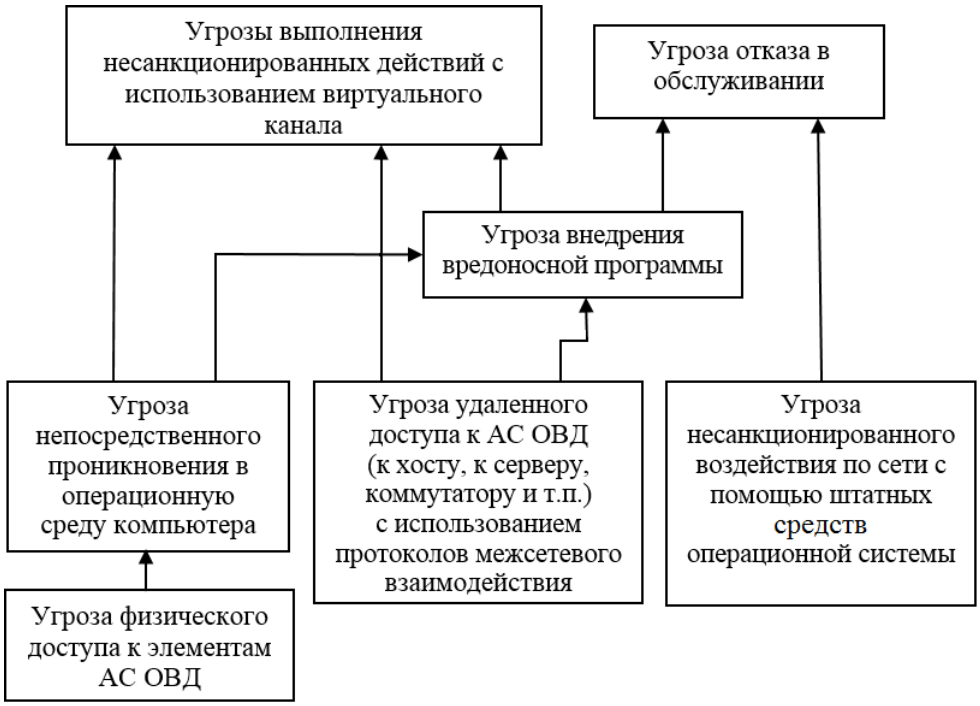

Рис. 2. Иерархия угроз НСД, направленных на нарушение ИБ АС на объекте информатизации ОВД (Fig. 2. The hierarchy of threats related to unauthorized access aimed to security violation of AS at the object of Informatization OVD)

С целью упорядочения представлений о разнообразии существующих информационных угроз неоднократно предпринимались попытки их классификации. В результате в литературе представлены разнообразные классификационные схемы, предназначенные, как правило, для решения конкретных практических задач [6, 7, 11–14]. Классификационная схема угроз, связанных с НСД к информационному ресурсу защищенной АС ОВД, представлена на рис. 3.

При рассмотрении вопроса функционирования АС в защищенном исполнении на объектах информатизации ОВД из всего множества угроз, связанных с НСД к служебной информации, определяющее значение имеют информационные угрозы, которые реализуются посредством удаленного взаимодействия с объектом воздействия (сетевых атак) [6, 11, 12].

В соответствии с [12] 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.

На рис. 4 представлены результаты проведенного в [15] анализа в виде процентного соотношения нарушений свойств информации в АС, на которые направлены сетевые атаки, применительно к объекту информатизации ОВД.

На основе анализа возможных объектов воздействия угроз, широко представленных в [15], и их связи с банком данных угроз БИ (bdu.fstec.ru), разработанным ФСТЭК России, уязвимостей компонентов и ПО АС на объектах информатизации ОВД с точки зрения реализации сетевых атак, определенных по итогам опроса экспертов в области обеспечения ИБ, выделены основные объекты воздействия сетевых атак на АС ОВД [13]: ПО, аппаратно-техническое обеспечение, оператор, каналы передачи данных.

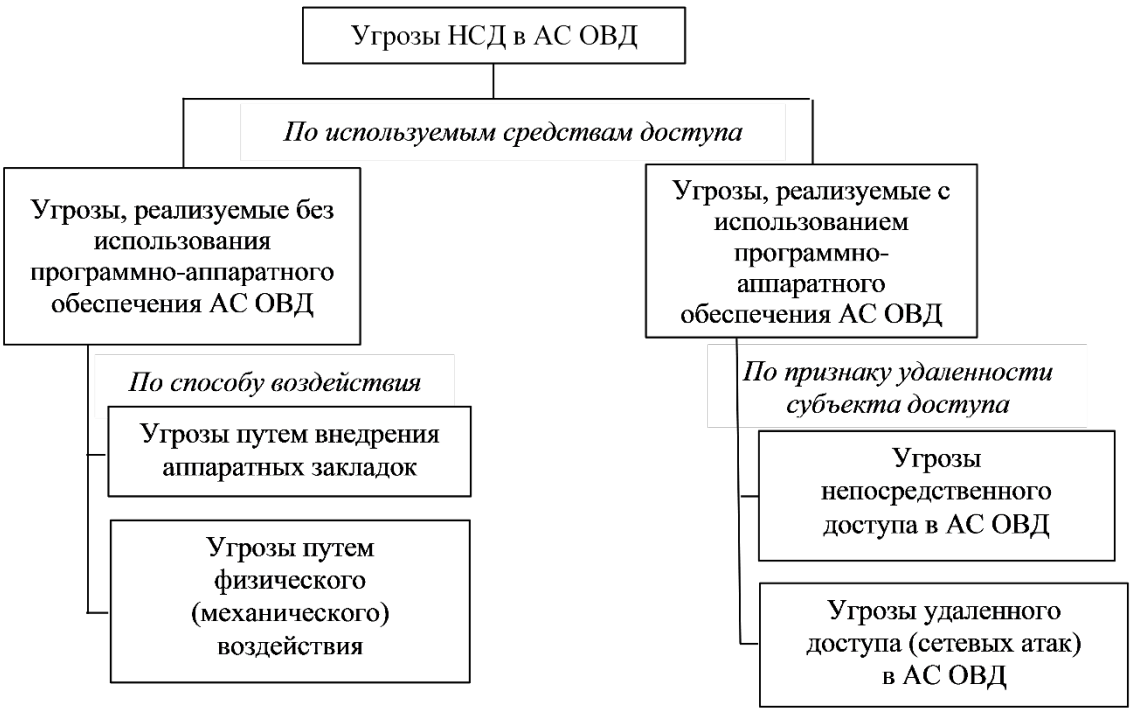

Рис. 3. Классификационная схема угроз, связанных с НСД к информационному ресурсу АС на объекте информатизации ОВД
(Fig. 3. Classification scheme of the threats related to unauthorized access to the information resource AS at the object of Informatization OVD)

Процесс реализации типовой сетевой атаки на информационный ресурс АС, связанный с персональными данными, подробно описан в [7]. В общем случае он включает в себя последовательное прохождение четырех этапов: сбор информации об объекте атаки; вторжение; реализация деструктивных действий; ликвидация следов атаки. В соответствии с данным описанием разработано содержание этапов типовой сетевой атаки на АС ОВД (рис. 5).

Рис. 4. Процентное соотношение нарушений свойств информации в результате воздействия сетевых атак на АС ОВД
(Fig. 4. The percentage fractions of information violations as a result of network attacks on ATS)

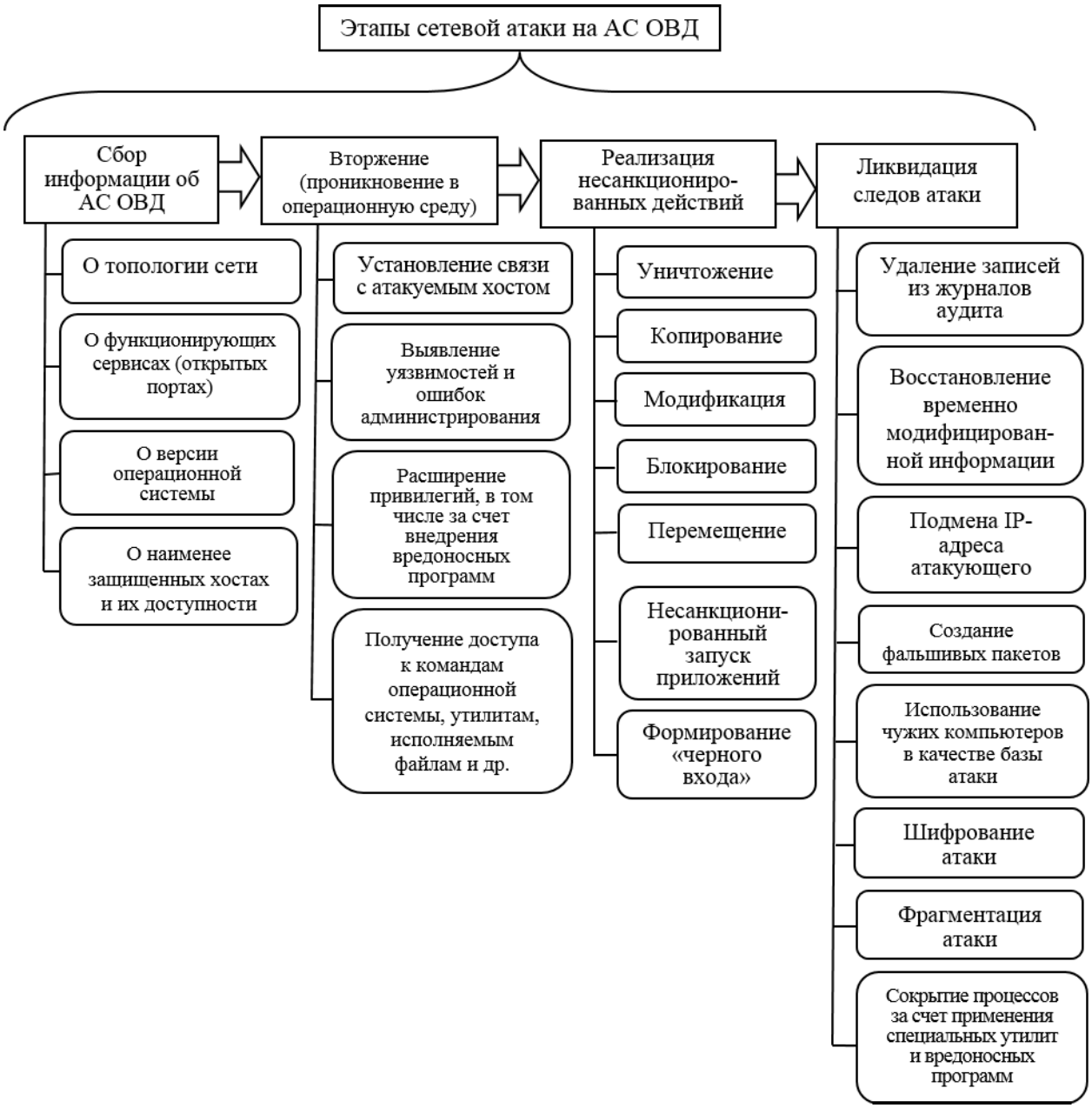

Рис. 5. Процесс реализации типовой сетевой атаки на АС ОВД
(Fig. 5. The process of implementing a typical network attack on ATS)

На рис. 6 представлена разработанная классификационная схема сетевых атак на АС ОВД, в которой система семи классификационных признаков, предложенная в [7] для телекоммуникационной сети, подключенной к глобальной сети Internet, использована в качестве основы для проведения классификации.

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, требований приказов и инструкций МВД России [3], нормативных документов и отраслевых стандартов ФСТЭК России, регламентирующих разработку и эксплуатацию АС в защищенном исполнении [5, 7, 9, 10], результатов опроса экспертов в области защиты конфиденциальной информации

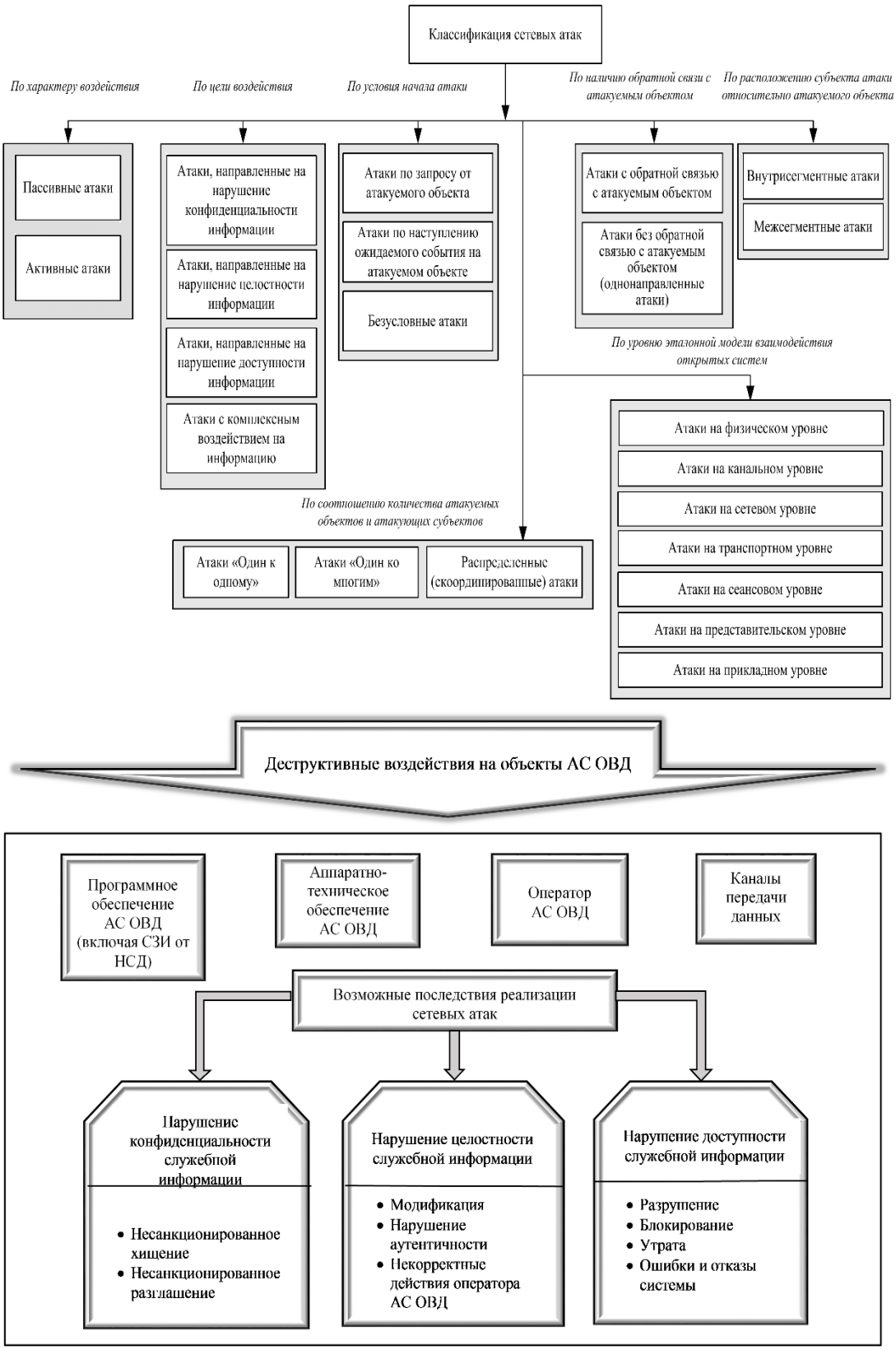

Рис. 6. Классификационная схема сетевых атак на АС на объекте информатизации ОВД (Fig. 6. Classification scheme of network attacks on the AS at the ATS Informatization facility)

позволил выделить восемь типов наиболее опасных и часто реализуемых в настоящее время сетевых атак на АС ОВД в соответствии с проведенной классификацией [6, 7, 11] с учетом возможных последствий их реализации (причиненного ущерба) (табл. 1).

Таблица 1. Перечень основных сетевых атак на АС на объекте информатизации ОВД

№ пп	Тип атаки	Шифр атаки	Название атаки
1	Анализ сетевого трафика	УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства служебной информации
		УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
		УБИ.117	Угроза перехвата привилегированного потока
		УБИ.118	Угроза перехвата привилегированного процесса
		УБИ.119	Угроза перехвата управления гипервизором
		УБИ.120	Угроза перехвата управления средой виртуализации
2	Сканирование сети	УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL
3	«Парольная» атака	УБИ.004	Угроза аппаратного сброса пароля BIOS
		УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени
		УБИ.207	Угроза НСД к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)
4	Подмена доверенного объекта сети	УБИ.086	Угроза несанкционированного изменения аутентификационной информации
		УБИ.128	Угроза подмены доверенного пользователя
		УБИ.188	Угроза подмены ПО
5	Навязывание ложного маршрута	УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
		УБИ.028	Угроза использования альтернативных путей доступа к ресурсам
6	Внедрение ложного объекта сети	УБИ.018	Угроза загрузки нештатной операционной системы
		УБИ.022	Угроза избыточного выделения оперативной памяти
		УБИ.023	Угроза изменения компонентов АС ОВД
		УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера
		УБИ.025	Угроза изменения системных и глобальных переменных
		УБИ.026	Угроза искажения XML-схемы
		УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации
		УБИ.124	Угроза подделки записей журнала регистрации событий
		УБИ.126	Угроза подмены беспроводного клиента или точки доступа
		УБИ.127	Угроза подмены действия пользователя путем обмана
		УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS
		УБИ.130	Угроза подмены содержимого сетевых ресурсов
		УБИ.131	Угроза подмены субъекта сетевого доступа
7	Отказ в обслуживании	УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных
		УБИ.106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера
		УБИ.107	Угроза отключения контрольных датчиков
		УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
		УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре
		УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации
8	Удаленный запуск приложений	УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы
		УБИ.212	Угроза перехвата управления АС ОВД

Заключение

В статье разработаны трехуровневая иерархия и классификационная схема угроз, связанных с несанкционированным доступом к информационному ресурсу автоматизированных систем органов внутренних дел и направленных на нарушение состояния их информационной безопасности.

Приведено содержание основных этапов типовой сетевой атаки, предложена классификационная схема сетевых атак на программное обеспечение и компоненты АС на объектах информатизации ОВД, разработанная с учетом семи классификационных признаков. В соответствии с проведенной классификацией сформирован перечень основных сетевых атак на АС ОВД, включающий восемь типов наиболее опасных и часто реализуемых в настоящее время атак.

Результаты анализа сетевых атак из сформированного перечня, их источников и объектов воздействия с учетом возможных деструктивных последствий реализации в АС ОВД, позволят провести количественную оценку опасности реализации атак, 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 защите информации 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.

СПИСОК ЛИТЕРАТУРЫ:

1. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646. URL:http://publication.pravo.gov.ru/Document/View/ 0001201612060002 (дата обращения: 14.11.2019).
2. 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: Воронеж. ин-т МВД России, 2015. – 92 с.
3. Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года: приказ МВД России от 14.03.2012 № 169. URL: http://policemagazine.ru/forum/ showthread.php?t=3663 (дата обращения: 27.10.2019).
4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. URL: http://docs.cntd.ru/document/1200058320 (дата обращения: 27.10.2019).
5. Руководящий документ Государственной технической комиссии от 30 июня 1992 года. Защита от несанкционированного доступа к информации. Термины и определения. URL: https://fstec.ru/component/attachments/download/298 (дата обращения: 13.11.2019).
6. Язов Ю.К. Защита информации в информационных системах от несанкционированного доступа / Ю.К. Язов, С.В. Соловьев. Воронеж: Кварта, 2015. – 440 с.
7. ФСТЭК России. Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка), 2008 год. URL: https://fstec.ru/component/ attachments/download/289 (дата обращения: 14.10.2019).
8. Методы и средства оценки защищенности автоматизированных систем органов внутренних дел: монография / Дровникова И.Г. и др. Воронеж: Воронеж. ин-т МВД России, 2017. – 88 с.
9. ГОСТР ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2: Функциональные компоненты безопасности. URL: http://docs.cntd.ru/document/1200105710 (дата обращения: 18.11.2019).
10. ГОСТ Р 51583-2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. URL: http://docs.cntd.ru/document/1200108858 (дата обращения: 11.11.2019).
11. 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.

12. Язов Ю.К. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. Воронеж: Кварта, 2018. – 588 с.
13. 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.
14. 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.
15. 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. проф. Н.Е. Жуковского и Ю.А. Гагарина, 2016. – 200 с.

REFERENCES:

[1] About the statement of the Doctrine of information security of the Russian Federation: the decree of the President of the Russian Federation of 05.12.2016 № 646. URL:http://publication.pravo.gov.ru/Document/View/0001201612060002 (accessed: 14.11.2019) (in Russian).
[2] Methods and tools for evolutionary and structural modeling in support of requirements for software systems of information protection: monograph Zmeev A.A. [and others]; under the editorship of E.A. Rogozin. Voronezh: Voronezh Institute of the Ministry of internal Affairs of Russia, 2015. – 92 p. (in Russian).
[3] About the statement of the Concept of ensuring information security of internal Affairs bodies of the Russian Federation till 2020: the order of the Ministry of internal Affairs of Russia of 14.03.2012 № 169. URL: http://policemagazine.ru/forum/showthread.php?t=3663 (accessed: 27.10.2019) (in Russian).
[4] GOST R 50922-2006. Information protection. Basic terms and definitions. URL: http://docs.cntd.ru/document/1200058320 (accessed 27.10.2019) (in Russian).
[5] Guidance document of the State technical Commission of June 30, 1992. Protection against unauthorized access to information. Terms and definitions. URL:https://fstec.ru/component/attachments/download/298 (accessed: 13.11.2019) (in Russian).
[6] Yazov Yu.K. Protection of information in information systems from unauthorized access Yu.K. Yazov, S.V. Soloviev. Voronezh: Kvarta, 2015. – 440 p. (in Russian).
[7] FSTEC of Russia. Methodical document. Basic model of threats to the security of personal data in their processing in information systems of personal data (extract), 2008. URL: https://fstec.ru/ component/attachments/download/289 (accessed: 14.10.2019) (in Russian).
[8] Methods and tools for assessing the security of automated systems of bodies of internal Affairs: monograph Drovnikova I.G. and others. Voronezh: Voronezh Institute of the Ministry of internal Affairs of Russia, 2017. – 88 p. (in Russian).
[9] GOST R ISO/IEC 15408-2-2013. Information technology. Methods and means of security. Information technology security assessment criteria. Part 2: Functional components of safety. URL: http://docs.cntd.ru/document/1200105710 (accessed: 18.11.2019) (in Russian).
[10] GOST R 51583-2014. National standard of the Russian Federation. Information protection. Order of creation of the automated systems in the protected execution. URL:http://docs.cntd.ru/document/1200108858 (accessed: 11.11.2019) (in Russian).
[11] Radko N.M. Penetration into the computer operating environment: models of malicious remote access N.M. Radko, Yu.K. Yazov, N.N. Korneeva. Voronezh: Voronezh. Govt. technical. UNT, 2013. – 265 p. (in Russian).
[12] Yazov Yu.K. Organization of information protection in information systems from unauthorized access: monograph Yu.K. Yazov, S.V. Soloviev. Voronezh: Kvarta, 2018. – 588 p. (in Russian).
[13] Popov A.D. Models and algorithms for evaluating the effectiveness of information protection systems against unauthorized access taking into account their temporal characteristics in automated systems of internal Affairs: dis. cand. tech. sciences: 05.13.19, Popov Anton Dmitrievich. Voronezh, 2018. – 163 p. (in Russian).
[14] Popov A.D. Classification of information security threats in automated information systems E.A. Rogozin, A.D. Popov, D.I. Korobkin. Devices and systems. Management, control, diagnostics. 2017. №. 7. P. 22–26. (in Russian).
[15] Application of new information technologies in the development of training complexes in the interests of the Armed forces of the Russian Federation: monograph Makhinov D.V. [and others]. Voronezh: VUNTS VVS «VVA» them. prof. N.E. Zhukovsky and Y.A. Gagarin, 2016. – 200 p. (in Russian).

Поступила в редакцию – 20 декабря 2019 г. Окончательный вариант – 05 февраля 2020 г.
Received – December 20, 2019. The final version – February 05, 2020.