Анна В. Бацких[1], Ирина Г. Дровникова[2], Евгений А. Рогозин[3]
[1,2,3]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: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

АНАЛИЗ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМ УПРАВЛЕНИЯ ДОСТУПОМ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И ОСНОВНЫЕ АСПЕКТЫ ИХ СОВЕРШЕНСТВОВАНИЯ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

DOI: http://dx.doi.org/10.26583/bit.2020.2.01

Аннотация. В статье представлены результаты анализа научно-технической литературы и открытых нормативно-распорядительных документов международного, федерального и ведомственного уровней, посвященных процессу функционирования систем защиты информации (СЗИ) от несанкционированного доступа (НСД) в автоматизированных системах (АС) на объектах информатизации органов внутренних дел (ОВД). На примере типовой сертифицированной СЗИ от НСД «Страж NT 4.0» рассмотрены функциональные возможности действующих в защищенных АС ОВД СЗИ от НСД, выявлены недостатки и определены основные аспекты совершенствования подсистем управления доступом данных систем на основе использования новых информационно-телекоммуникационных технологий, связанных с повышением реальной защищенности АС на объектах информатизации ОВД. В качестве перспективной технологии предложена дополнительная биометрическая аутентификация, основанная на распознавании субъекта доступа по индивидуальной динамике клавиатурного набора (клавиатурному почерку).
Ключевые слова: защита информации, система защиты информации, подсистема управления доступом, несанкционированный доступ, аутентификация пользователя, клавиатурный почерк.
Для цитирования: БАЦКИХ, Анна В.; ДРОВНИКОВА, Ирина Г.; РОГОЗИН, Евгений А. АНАЛИЗ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМ УПРАВЛЕНИЯ ДОСТУПОМ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И ОСНОВНЫЕ АСПЕКТЫ ИХ СОВЕРШЕНСТВОВАНИЯ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 6-17, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1267>. Дата доступа: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.01.

Anna V. Batskih[1], Irina G. Drovnikova[2], Evgeni A. Rogozin[3]
[1,2,3]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: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

Analysis of the process of functioning of subsystems of access control systems to protect information from unauthorized access and basic aspects their perfection in automated systems of internal affairs bodies

DOI: http://dx.doi.org/10.26583/bit.2020.2.01

Abstract. The paper presents the results of the analysis of scientific and technical literature and open regulatory and administrative documents of the international, Federal and departmental levels devoted to the process of functioning of information protection systems (SPI) from unauthorized access (UA) in automated systems (AS) at the objects of Informatization of internal Affairs bodies (ATS). Using the

example of a typical certified SPI from UA «Strazh NT 4.0» the functionality of SPI from UA operating in protected ATS is analyzed, shortcomings are identified and the key aspects of improving subsystems of access control systems based on the use of new information and telecommunication technologies related to improving real security as on the objects of Informatization Department are defined. As a promising technology additional biometric authentication based on realization of recognition of the access subject on individual dynamics of a keyboard set (keyboard handwriting) is offered.
Keywords: information protection, information security system, access control subsystem, unauthorized access, authenticate users, keyboard handwriting.
For citation: BATSKIH, Anna V.; DROVNIKOVA, Irina G.; ROGOZIN, Evgeni A. Analysis of the process of functioning of subsystems of access control systems to protect information from unauthorized access and basic aspects their perfection in automated systems of internal affairs bodies. IT Security (Russia), [S.l.], v. 27, n. 2, p. 6-17, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1267>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.01.

Введение

Характерной особенностью настоящего времени является ускоренный темп развития новых информационно-телекоммуникационных технологий и их широкое проникновение практически во все сферы человеческой деятельности. Это активно используется различного рода злоумышленниками, несанкционированное воздействие которых на информационный ресурс АС приводит к нарушению целостности, конфиденциальности или доступности хранящейся, обрабатываемой и передаваемой информации и в результате – к нарушению надежности функционирования АС в целом по ее прямому назначению. Согласно статистическим данным Генеральной прокуратуры Российской Федерации отмечается ежегодный рост преступлений, связанных с использованием информационно-коммуникационных технологий: по итогам за январь–август 2019 года число преступлений в сфере компьютерной информации выросло более чем в полтора раза (+66,8 %), правоохранители выявили 180 153 преступления [1]. В результате таких преступных действий наносится ощутимый ущерб объектам информатизации, эксплуатирующим АС различного назначения. Это в первую очередь относится к АС на объектах информатизации критического применения, характеризующихся неприемлемыми для народного хозяйства размерами ущерба, а также других последствий, возникающих по причине нарушения их работоспособности, сбоев или отказов в работе. К такого рода объектам в полной мере следует отнести и объекты информатизации, эксплуатирующие АС ОВД.

Динамика киберпреступности диктует необходимость повышения эффективности противодействия ей, что относится к стратегическим направлениям деятельности правоохранительных органов. Таким образом, вопросы, связанные обеспечением надежности функционирования АС на объектах информатизации ОВД и, в частности, их информационной безопасности (ИБ), являются весьма актуальными. Их актуальность основывается на основных положениях Доктрины ИБ, в которой отмечается необходимость как повышения защищенности критической информационной структуры и устойчивости ее функционирования, так и развития механизмов обнаружения, защиты и предупреждения информационных угроз [2]. Концепция обеспечения информационной безопасности ОВД Российской Федерации до 2020 года определяет комплекс мер, направленных на обеспечение защиты информации (ЗИ), информационных ресурсов и информационных систем ОВД Российской Федерации от специальных программно-технических воздействий, средств технических разведок, НСД, а также утечки информации по техническим каналам [3].

Опыт эксплуатации современных АС ОВД показал, что наибольший вклад в нарушение надежности их функционирования вносят угрозы, связанные с НСД к

конфиденциальному информационному ресурсу [4, 5]. С целью ЗИ от НСД используют СЗИ от НСД – важнейшую и обязательную составляющую механизма защиты современных АС на объектах информатизации ОВД [6]. Одной из ключевых функций СЗИ от НСД является управление доступом к информации, реализуемой ее важнейшей подсистемой – подсистемой управления доступом [7]. Результаты проведенного в [4] анализа эффективности функционирования СЗИ в АС, функционирующих в защищенном исполнении на объектах информатизации ОВД, с учетом современной мировой тенденции приоритетного развития средств аутентификации в программных продуктах ИБ [8, 9], требований руководящих документов Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [7] и нормативных актов МВД России [3] позволяет сделать вывод об актуальности задач разработки новых подсистем управления доступом в СЗИ от НСД защищенных АС ОВД или усиления уже существующих подсистем путем объединения стандартной процедуры аутентификации с процедурой дополнительной аутентификации субъектов доступа на основе использования современных информационно-телекоммуникационных технологий (в первую очередь, при обращении к особо важному информационному ресурсу).

1. Постановка задачи

Для определения основных аспектов совершенствования действующих подсистем управления доступом СЗИ от НСД в АС ОВД необходимо решить следующие задачи:

1. На основе результатов анализа открытой нормативно-распорядительной документации международного, федерального и ведомственного уровней, регламентирующей разработку и эксплуатацию АС ОВД в защищенном исполнении, определить основные направления формирования требований, предъявляемых к функционированию их СЗИ от НСД.

2. Рассмотреть состав СЗИ от НСД в АС ОВД и определить базовые функции ее подсистемы управления доступом.

3. Раскрыть назначение и основные функции типовой широко используемой в защищенных АС ОВД СЗИ от НСД «Страж NT 4.0», провести ее классификацию по условиям функционирования с точки зрения ЗИ в АС на объектах информатизации ОВД для уточнения требований, предъявляемых к подсистеме управления доступом, с целью разработки и применения обоснованных мер по достижению требуемого уровня защищенности служебной информации.

4. Выявить недостатки функционирования подсистемы управления доступом СЗИ от НСД «Страж NT 4.0» на объектах информатизации ОВД с целью определения функциональных возможностей подсистемы и направлений ее совершенствования для достижения требуемого уровня ЗИ.

2. Теоретический анализ

Анализ международных и отраслевых стандартов Российской Федерации по ИБ АС [8–10], Руководящих документов ФСТЭК России [5–7, 11–13], а также ведомственных нормативных актов по вопросам ЗИ на объектах информатизации ОВД [3] показал, что оценка эффективности функционирования систем и средств ЗИ на этапе эксплуатации АС и разработка адекватных существующим угрозам перспективных образцов этих систем является одним из важнейших моментов в процессе эксплуатации АС ОВД в защищенном исполнении. Следовательно, оценка эффективности СЗИ от НСД в АС ОВД может быть положена в основу формирования требований по ЗИ в данных системах.

Результаты анализа нормативно-распорядительных документов, используемых для

оценки эффективности СЗИ от НСД в АС ОВД [2, 3, 5, 10, 14–22], подробно представленные в [4, 23, 24], показали:

– необходимость доработки существующих в настоящее время требований по ЗИ в АС ОВД, основанных на функциональных требованиях к оценке эффективности СЗИ от НСД без учета поведения данных систем в динамическом (временном) диапазоне;

– необходимость совершенствования существующих СЗИ в АС ОВД в направлении управления процессами ЗИ от НСД с помощью управляемых параметров на основе количественной оценки эффективности функционирования СЗИ от НСД.

В соответствии с [6] СЗИ от НСД представляет собой комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от НСД к информации в АС. Применительно к объекту информатизации ОВД СЗИ от НСД следует рассматривать как функционально самостоятельную подсистему всех необходимых мероприятий, методов и средств, выделяемых (предусматриваемых) в АС ОВД с целью решения актуальных задач ЗИ от НСД. Программные средства ЗИ, входящие в состав СЗИ от НСД АС ОВД, образуют отдельную ее подсистему, обладающую рядом достоинств: надежностью, гибкостью, универсальностью, возможностью модификации и развития, простотой реализации [25]. Это позволяет совершенствовать существующие СЗИ на объектах информатизации ОВД для обеспечения требуемого уровня защищенности служебной информации от угроз НСД, повышая при этом общую надежность функционирования АС ОВД в защищенном исполнении.

На основе анализа структур СЗИ от НСД, действующих в защищенных АС на объектах информатизации ОВД [4, 26], и руководящих документов [7, 9] определено, что типовая СЗИ от НСД АС ОВД включает в свой состав пять основных подсистем: подсистему управления доступом («Включение ПК и идентификация пользователя»), подсистему разграничения доступа («Инициализация прав пользователя на работу в системе и доступ к каталогу файлов»), подсистему регистрации и учета («Работа пользователя с файлами и программами»), криптографическую подсистему («Работа пользователя с прикладным программным обеспечением»), подсистему обеспечения целостности («Деструктивное воздействие на СЗИ от НСД»).

В соответствии с [7] к базовым функциям подсистемы управления доступом СЗИ от НСД АС ОВД относятся идентификация и аутентификация (проверка подлинности) субъектов доступа.

Согласно [6] идентификация понимается как присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов, а аутентификация – как проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности. Посредством идентификации субъекту доступа (пользователю, действующему от имени определенного пользователя процессу, другому аппаратно-программному компоненту) предоставляется возможность сообщать свое имя (назвать себя). Аутентификация позволяет другой стороне убеждаться в том, что субъект доступа действительно является тем, за кого себя выдает. Основными методами аутентификации субъектов доступа в настоящее время являются: парольная аутентификация, маркеры аутентификации (смарт-карты), биометрическая аутентификация [27].

Парольная аутентификация осуществляется с использованием устройств идентификации и проверки подлинности субъекта доступа, представляющих собой USB-устройства, на которых записываются персональные данные субъекта доступа, позволяющие СЗИ от НСД по введенному вручную паролю определить данного субъекта и его привилегии входа в систему. Основными достоинствами парольной аутентификации

являются ее простота и привычность, связанные со встроенностью паролей в современные операционные системы и другие сервисы, что при правильном использовании паролей позволяет обеспечить приемлемый во многих случаях уровень ИБ. В то же время парольную аутентификацию следует признать самым слабым средством проверки подлинности по совокупности характеристик (ограничения на длину пароля, связанные с ограниченностью человеческой памяти; влияние длины пароля на время аутентификации и др.).

Более надежной альтернативой паролям можно считать маркеры аутентификации (смарт-карты), однако использование данного метода аутентификации связано с серьезными дополнительными расходами и не исключает возможности маскировки нарушителя под легального пользователя АС в случае утери или кражи смарт-карты. Смарт-карты также не способны предотвратить сетевую атаку с использованием уязвимых мест, поскольку рассчитаны на правильный вход субъекта доступа в систему.

Наиболее точной технологией аутентификации субъектов доступа является биометрическая аутентификация. Биометрия представляет собой комплекс автоматизированных методов аутентификации человека, основанных на анализе его физиологии (отпечатки пальцев, сетчатка и роговица глаз, геометрия руки и лица и др.) и поведения (динамика ручной подписи, стиль работы с клавиатурой). На стыке физиологических особенностей и поведенческих характеристик находятся анализ особенностей голоса и распознавание речи [27].

3. Обсуждение результатов

Для ЗИ на объектах информатизации, эксплуатирующих защищенные АС ОВД, в настоящее время используются СЗИ от НСД «Dallas Lock», «Dallas Lock Linux», «Secret Net», «Secret Net Studio», «Страж NT» и др. Наиболее широкое применение в АС ОВД для защиты конфиденциальной информации и сведений, составляющих государственную тайну, нашла СЗИ от НСД «Страж NT 4.0», на примере которой рассмотрим функциональные возможности СЗИ от НСД, действующих в АС ОВД, выявим существующие недостатки их функционирования для определения направлений совершенствования подсистем управления доступом данных систем с целью повышения реальной защищенности АС на объектах информатизации ОВД.

СЗИ от НСД «Страж NT 4.0» является сертифицированным (сертификат ФСТЭК России № 3553, выдан 20.04.2016, действует до 20.04.2024) программным средством защиты от НСД к информации и соответствует требованиям руководящих документов [11] по 3-му классу защищенности средств вычислительной техники (СВТ) и [13] по 2-му уровню контроля отсутствия недекларированных возможностей. Она предназначена для комплексной защиты информационных ресурсов от НСД в соответствии с требованиями законодательства Российской Федерации: в АС до класса защищенности 1Б включительно, в государственных информационных системах до 1-го класса защищенности включительно, в информационных системах персональных данных до 1-го уровня защищенности включительно. Функционирует в среде 32-х и 64-разрядных операционных систем Microsoft Windows, поддерживая новейшие версии Microsoft до Windows 10 включительно (в АС ОВД используются версии Microsoft до Windows 7 включительно).

СЗИ от НСД «Страж NT 4.0» обладает рядом ощутимых преимуществ по сравнению с ее предыдущими версиями и представляет собой многофункциональную систему, реализующую следующие основные функции [28, 29]:

– двухфакторная аутентификация до загрузки операционной системы (в том числе и для виртуальной среды) с использованием аппаратных идентификаторов (USB-идентификаторов типа Guardant ID, Rutoken, eToken, JaCarta, ESMART Token) и смарт-карт

(Рутокен, eToken, JaCarta, ESMART);

– дискреционный и мандатный принципы контроля доступа к ресурсам системы;

– создание замкнутой программной среды пользователя, позволяющей ему запуск только разрешенных приложений;

– регистрация событий безопасности, в том числе и действий администратора.

– маркировка выдаваемых на печать документов независимо от печатающего их приложения;

– гарантированная очистка;

– контроль целостности защищаемых ресурсов и компонентов СЗИ;

– управление пользователями, носителями информации и устройствами;

– преобразование информации на отчуждаемых носителях;

– тестирование СЗИ.

Проведем классификацию СЗИ от НСД «Страж NT 4.0» по условиям ее функционирования с точки зрения ЗИ в АС ОВД для уточнения требований идентификации и аутентификации субъектов доступа, предъявляемых к подсистеме управления доступом.

Для подсистемы управления доступом СЗИ от НСД «Страж NT 4.0» АС ОВД класса защищенности 1Б в соответствии с пп. 2.10, 2.14 Руководящего документа ФСТЭК России [7] должны быть реализованы требования идентификации и аутентификации, представленные в таблице 1.

Для используемой в АС ОВД подсистемы управления доступом СЗИ от НСД «Страж NT 4.0», сертифицированной по 3-го классу защищенности СВТ, в соответствии с руководящим документом [11] должны выполняться требования к показателям защищенности в части идентификации и аутентификации, представленные в таблице 2.

Результаты исследования качества функционирования подсистем управления доступом СЗИ от НСД современных защищенных АС ОВД, представленные в [4, 25], показали: их высокую значимость в решении проблемы ЗИ на объектах информатизации, эксплуатирующих данные системы, особенно в условиях возрастания угроз НСД; зависимость сложности целесообразных для применения в АС ОВД процедур и средств идентификации и аутентификации субъектов доступа от уровня конфиденциальности защищаемой служебной информации; важность проведения контроля физического состояния субъекта доступа к информационному ресурсу высокого уровня конфиденциальности в процессе аутентификации, поскольку его ошибочные действия могут привести к потерям, неприемлемым для ОВД и общества в целом.

Результаты проведенной классификации СЗИ от НСД «Страж NT 4.0» по условиям ее функционирования с точки зрения ЗИ в АС ОВД, а также результаты изучения опыта эксплуатации СЗИ от НСД «Страж NT 4.0» в защищенных АС на объектах информатизации ОВД с осуществлением стандартных процедур идентификации и аутентификации субъектов доступа, основанных на парольной аутентификации и использовании смарт-карт, представленные в [30], позволяют констатировать, что функциональные возможности подсистемы управления доступом СЗИ от НСД «Страж NT 4.0», определяемые требованиями действующей нормативно-распорядительной документации, датированной 1992 годом [7, 11], не соответствуют как возможностям современных АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД, так и потребности подразделений ОВД, занимающихся обработкой конфиденциальной информации. Следовательно данная подсистема нуждается в существенной доработке на основе применения новых информационно-телекоммуникационных технологий в области ЗИ для достижения требуемого уровня защищенности служебной информации без нарушения эффективности функционирования АС ОВД по прямому назначению. В первую очередь это

касается особо важного информационного ресурса, требующего повышенной защищенности (информация высокого уровня конфиденциальности, наиболее важные параметры функционирования АС ОВД и др.). Как правило данный информационный ресурс предназначен для узкого круга санкционированных субъектов доступа и характеризуется малой частотой обращений к нему.

Таблица 1. Требования к подсистеме управления доступом СЗИ от НСД «Страж NT 4.0» АС ОВД по идентификации и аутентификации субъектов доступа в соответствии с [7]

Наличие/отсутствие требований	Требования	Расшифровка требований
+	Идентификация, аутентификация субъектов доступа в систему	Идентификация и аутентификация субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия длиной не менее восьми буквенно-цифровых символов
+	Идентификация, аутентификация субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	Идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по физическим адресам (номерам)
+	Идентификация, аутентификация субъектов доступа к программам	Идентификация программ по именам
+	Идентификация, аутентификация субъектов доступа к томам, каталогам, файлам, записям, полям записей	Идентификация программ, томов, каталогов, файлов, записей, полей записей по именам

Обозначения: «–» – требования отсутствуют; «+» – есть требования.

Таблица 2. Требования к показателям защищенности подсистемы управления доступом СЗИ от НСД «Страж NT 4.0» АС ОВД в части идентификации и аутентификации в соответствии с [11]

Наличие/отсутствие требований	Наименование показателя защищенности	Требования
=	Идентификация и аутентификация	Требование от субъектов доступа идентифицировать себя при запросах на доступ, проверка подлинности идентификатора субъекта — осуществление аутентификации. Подсистема должна располагать необходимыми данными для идентификации н аутентификации и препятствовать входу в систему неиденфицированного субъекта или субъекта, подлинность которого при аутентификации не подтвердилась. Подсистема должна обладать способностью надежно связывать полученную идентификацию со всеми действиями данного субъекта доступа.

Обозначения: «–» – требования отсутствуют; «+» – новые либо дополнительные требования; «=» – требования совпадают с требованиями к СВТ предыдущего класса.

Управление эффективностью функционирования подсистемы управления доступом СЗИ от НСД для достижения требуемого уровня ЗИ в АС ОВД может быть осуществлено за счет усложнения процедуры аутентификации субъектов доступа и сокращения

необходимого для ее реализации временного диапазона. Поэтому с целью повышения защищенности АС, эксплуатируемых на объектах информатизации ОВД, предлагается при обращении к особо важному информационному ресурсу использовать подсистему многоуровневого управления доступом в систему, выполняющую помимо стандартной процедуры аутентификации субъектов доступа процедуру их дополнительной аутентификации. Это наиболее значимо для многопользовательских АС ОВД, относящихся к первой группе классов защищенности от НСД [7], имеющих широкую номенклатуру субъектов доступа с разными полномочиями к конфиденциальному информационному ресурсу, способных одновременно обрабатывать и (или) хранить информацию различных уровней конфиденциальности.

Перспективным направлением реализации процедуры дополнительной аутентификации может стать использование биометрической технологии, основанной на распознавании субъекта доступа к информационному ресурсу АС ОВД по индивидуальной динамике клавиатурного набора (клавиатурному почерку). Целесообразность применения аутентификации субъектов доступа по клавиатурному почерку по сравнению с другими технологиями биометрической аутентификации объясняется ее основными достоинствами: достаточно высокая степень эффективности, возможность контроля физического состояния субъектов доступа, скрытость использования, быстродействие, простота реализации и дешевизна [31, 32].

Заключение

Таким образом, в статье на основе анализа открытой разно уровневой нормативно–распорядительной документации, регламентирующей разработку и эксплуатацию АС ОВД в защищенном исполнении, определен состав СЗИ от НСД данных систем и выявлены основные направления формирования требований к их функционированию на объектах информатизации ОВД.

Раскрыты назначение, основные функции и проведена классификация типовой широко используемой в АС ОВД СЗИ от НСД «Страж NT 4.0» по условиям ее функционирования с точки зрения ЗИ. На основе проведенной классификации и изучения опыта эксплуатации СЗИ от НСД «Страж NT 4.0» в защищенных АС на объектах информатизации ОВД определены недостатки стандартной процедуры аутентификации и возможности ее совершенствования путем введения процедуры дополнительной биометрической аутентификации субъектов доступа по клавиатурному почерку для достижения требуемого уровня ЗИ.

Использование в типовых СЗИ от НСД защищенных АС на объектах информатизации ОВД подсистем многоуровневого управления доступом, основанных на реализации совокупной процедуры аутентификации субъектов доступа, при обращении к особо важному информационному ресурсу позволит обеспечить высокий уровень защищенности АС ОВД от угроз НСД к служебной информации указанного уровня конфиденциальности, не нарушая при этом требуемой эффективности ее функционирования по прямому назначению.

СПИСОК ЛИТЕРАТУРЫ:

1. Статистические данные о зарегистрированных преступлениях на территории Российской Федерации в январе–августе 2019 года. URL: https://www.genproc.gov.ru/smi/news/genproc/news–1703326/ (дата обращения: 20.11.2019).
2. 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: 14.12.2019).
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: 28.11.2019).
4. 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.
5. ФСТЭК России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. URL: https://fstec.ru/component/attachments/download/299 (дата обращения: 13.12.2019).
6. ФСТЭК России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. URL: https://fstec.ru/component/attachments/download/298 (дата обращения: 13.12.2019).
7. ФСТЭК России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. URL: https://fstec.ru/component/attachments/download/296 (дата обращения: 14.12.2019).
8. ISO/IEC 15408. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1 Revision 4, September 2012. – 93 p. URL: https://commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf (дата обращения: 10.12.2019).
9. ГОСТ Р 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: 10.12.2019).
10. ГОСТ Р 51583–2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. URL: http://docs.cntd.ru/document/1200108858 (дата обращения: 11.12.2019).
11. ФСТЭК России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. 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: 11.12.2019).
12. ФСТЭК России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. URL: http://docs.cntd.ru/document/901817221 (дата обращения: 28.11.2019).
13. ФСТЭК России. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1: Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. URL: http://meganorm.ru/Index2/1/4293808/4293808514.htm (дата обращения: 28.11.2019).
14. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149–ФЗ (в ред. от 19.12.2016) (с изм. и доп., вступ. в силу с 13.12.2019). URL: https://legalacts.ru/doc/FZ–ob–informacii–informacionnyh–tehnologijah–i–o–zawite–informacii/ (дата обращения: 02.12.2019).
15. О государственной тайне: закон Российской Федерации от 21.07.1993 № 5485–1 (в ред. от 08.03.2015) // СПС «КонсультантПлюс» (дата обращения: 12.12.2019).
16. О сертификации средств защиты информации: постановление Правительства РФ от 26.06.1995 № 608 (ред. от 21.04.2010) // СПС «КонсультантПлюс» (дата обращения: 03.12.2019).
17. Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну…: постановление Правительства РФ от 21.04.2010 № 266 (в ред. от 03.11.2014) // СПС «КонсультантПлюс» (дата обращения: 10.12.2019).
18. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. URL: http://docs.cntd.ru/document/gost–r–50922–2006 (дата обращения: 02.12.2019).

19. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения // СПС «КонсультантПлюс» (дата обращения: 10.12.2019).
20. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18.02.2013 № 21 (в ред. от 23.03.2017) // СПС «КонсультантПлюс» (дата обращения: 02.12.2019).
21. Об утверждении Наставления по технической защите информации в системе Министерства внутренних дел: приказ МВД России от 06.03.2013 № 010.
22. ГОСТ Р 53114–2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. URL: http://docs.cntd.ru/document/1200075565 (дата обращения: 02.12.2019).
23. Каднова А.М. Система показателей качества функционирования при создании системы информационной безопасности на объекте информатизации ОВД / О.И. Бокова, А.М. Каднова, Е.А. Рогозин, А.С. Серпилин // Приборы и системы, управление, контроль, диагностика. 2019. № 1. С. 26–33.
24. Каднова, Айжана М. et al. Алгоритм создания автоматизированных систем в защищенном исполнении. Безопасность информационных технологий, [S.l.], Т. 26, № 4. С. 93–100, dec. 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1235> (дата обращения: 12.12.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.07.
25. Формирование требований к системам защиты информации от несанкционированного доступа в автоматизированные системы органов внутренних дел на основе генетического алгоритма: монография / Дровникова И.Г. [и др.]. Воронеж: Воронеж. ин-т МВД России, 2019. – 128 с.
26. Бокова, Оксана И. Et al. Разработка имитационной модели системы защиты информации от несанкционированного доступа с использованием программной среды cpn tools. Безопасность информационных технологий, [S.l.], Т. 26, № 3. С. 80–89, sep. 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1220> (дата обращения: 12.12.2020). DOI: http://dx.doi.org/10.26583/bit.2019.3.07.
27. Мартынова Л.Е. Исследование и сравнительный анализ методов аутентификации / Мартынова Л.Е. [и др.] // Молодой ученый. 2016. № 19. С. 90–93.
28. Система защиты информации от несанкционированного доступа «Страж NT 4.0». URL: https://www.guardnt.ru/gnt_40.html (дата обращения: 30.11.2019).
29. Страж NT. Система защиты информации от несанкционированного доступа. Версия 4.0. Руководство администратора. URL: https://labvs.ru/upload/iblock/390/390a1a477039748 e3f745132c08172a6.pdf (дата обращения: 30.11.2019).
30. Рогозин Е.А. Проблемы и пути их решения при проектировании систем защиты информации от несанкционированного доступа в автоматизированных информационных системах ОВД / Е.А. Рогозин, А.Д. Попов, Т.В. Мещерякова // Информационные технологии, связь и защита информации МВД России. 2017. Ч. 1. С. 115–118.
31. Аверин А.И. Аутентификация пользователей по клавиатурному почерку / А.И. Аверин, Д.П. Сидоров. URL: http://cyberleninka.ru/article/n/autentifikatsiya–polzovateley–po–klaviaturnomu–pocherku (дата обращения: 02.12.2019).
32. Яндиев И.Б. Исследование временных характеристик клавиатурного почерка для быстрой аутентификации личности / И.Б. Яндиев // Молодой ученый. 2017. № 14. С. 154–157.

REFERENCES:

[1] Statistical data on registered crimes in the territory of the Russian Federation in January–August. URL: https://www.genproc.gov.ru/smi/news/genproc/news–1703326/ (accessed: 20.11.2019) (in Russian).
[2] 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: 14.12.2019) (in Russian).
[3] About the statement of the Concept of ensuring information security of law–enforcement 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: 28.11.2019) (in Russian).
[4] 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).
[5] FSTEC of Russia. Guidance document. The concept of protection of computer equipment and automated systems from unauthorized access to information. URL: https://fstec.ru/component/attachments/ download/299 (accessed: 13.12.2019) (in Russian).

[6] FSTEC of Russia. Guidance document. Protection against unauthorized access to information. Terms and definitions. URL:https://fstec.ru/component/attachments/download/298 (accessed: 13.12.2019) (in Russian).
[7] FSTEC of Russia. Guidance document. Automated system. Protection against unauthorized access to information. Classification of automated systems and information security requirements. URL: https://fstec.ru/component/attachments/download/ 296 (accessed: 14.12.2019) (in Russian).
[8] ISO/IEC 15408. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1 Revision 4, September 2012. – 93 p. URL: https://commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf (accessed: 10.12.2019).
[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: 10.12.2019) (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: 11.12.2019) (in Russian).
[11] FSTEC of Russia. Guidance document. Computer aids. Protection against unauthorized access to information. Indicators of protection against unauthorized access to information. URL: http://fstec.ru/ tekhnicheskaya–zashchita–informatsii/dokumenty/114–spetsialnye–normativnye–dokumenty/383–rukovodyashchij– dokument–reshenie–predsedatelya–gostekhkomissii–rossii–ot–25–iyulya–1997–g (accessed: 11.12.2019) (in Russian).
[12] FSTEC of Russia. Guidance document. Temporary position on the organization of development, production and operation of software and technical means of information protection from unauthorized access in automated systems and computer equipment. URL: http://docs.cntd.ru/document/901817221 (accessed: 28.11.2019) (in Russian).
[13] FSTEC of Russia. Guidance document. Protection against unauthorized access to information. Part 1: information security software. Classification by the level of control of the absence of undeclared opportunities. URL: http://meganom.ru/Index2/1/4293808/4293808514.htm (accessed: 28.11.2019) (in Russian).
[14] On information, information technologies and information protection: Federal law № 149–FZ of 27.07.2006 (as amended on 19.12.2016) (with ed. and extra, intro. effective from 13.12.2019). URL:https://legalacts.ru/doc/FZ–ob–informacii–informacionnyh–tehnologijah–i–o–zawite–informacii/ (accessed: 02.12.2019) (in Russian).
[15] On state secrets: law of the Russian Federation № 5485–1 of 21.07.1993 (as amended on 08.03.2015). SPS «ConsultantPlus» (accessed: 12.12.2019) (in Russian).
[16] On certification of information security tools: decree of the Government of the Russian Federation of 26.06.1995 № 608 (ed. of 21.04.2010) SPS «ConsultantPlus» (accessed: 03.12.2019) (in Russian).
[17] About features of conformity assessment of products (works, services) used for protection of information constituting a state secret...: resolution of the Government of the Russian Federation of 21.04.2010 № 266 (as amended from 03.11.2014) SPS «ConsultantPlus» (accessed: 10.12.2019) (in Russian).
[18] GOST R 50922–2006. Information protection. Basic terms and definitions. URL: http://docs.cntd.ru/document/gost–r–50922–2006 (accessed: 02.12.2019) (in Russian).
[19] GOST R 51275–2006. Information protection. Object of Informatization. Factors that affect information. Generalities. SPS «ConsultantPlus» (accessed: 10.12.2019) (in Russian).
[20] On approval of the composition and content of organizational and technical measures to ensure the security of personal data when they are processed in personal data information systems: order of the FSTEC of Russia dated 18.02.2013 № 21 (as amended on 23.03.2017) SPS «ConsultantPlus» (accessed: 02.12.2019) (in Russian).
[21] About the approval of the Instruction on technical protection of information in the system of the Ministry of internal Affairs: order of the Ministry of internal Affairs of Russia of 06.03.2013 № 010 (in Russian).
[22] GOST R 53114–2008 information Protection. Ensuring information security in the organization. Basic terms and definitions. URL: http://docs.cntd.ru/document/ 1200075565 (accessed: 02.12.2019) (in Russian).
[23] Kadnova A.M. System of indicators of the quality of functioning when creating an information security system on the object of informatization of ATS. O.I. Bokova, A.M. Kadnova, E.A. Rogozin, A.S. Serpilin. Devices and systems, management, control, diagnostics. 2019. № 1. P. 26–33 (in Russian).
[24] Kadnova, Aizhana M. et al. Algorithm for creation of automated systems in protected performance. IT Security (Russia), [S.l.], v. 26, n. 4. P. 93–100, dec. 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1235> (accessed: 12.12.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.07.
[25] Formation of requirements to information protection systems from unauthorized access to automated systems of internal Affairs bodies on the basis of genetic algorithm: monograph Drovnikova I.G. [and others]. – Voronezh: Voronezh. Institute of MIA of Russia, 2019. – 128 p. (in Russian).
[26] Bokova, Oksana I. et al. Development of an imitation model of information protection system from unauthorized access using the cpn tools software. IT Security (Russia), [S.l.], v. 26, n. 3. P. 80-89, sep. 2019. ISSN 2074-7136.

URL: https://bit.mephi.ru/index.php/bit/article/view/1220 (accessed: 12.12.2020). DOI: http://dx.doi.org/10.26583/bit.2019.3.07 (in Russian).

[27] Martynova L.E. Research and comparative analysis of authentication methods Martynova L.E. [and others]. Young scientist. 2016. № 19. P. 90–93 (in Russian).

[28] Information protection system from unauthorized access «Strazh NT 4.0». URL:https://www.guardnt.ru/gnt_40.html (accessed: 30.11.2019) (in Russian).

[29] Strazh NT. The system of information protection from unauthorized access. Version 4.0. Administrator's guide. URL:https://labvs.ru/upload/iblock/390/390a1a477039748 e3f745132c08172a6.pdf (accessed: 30.11.2019) (in Russian).

[30] Rogozin E. A. Problems and ways to solve them when designing information protection systems from unauthorized access in automated information systems of the police Department E.A. Rogozin, A.D. Popov, T.V. Meshcheryakova. Information technologies, communication and information protection of the Ministry of internal Affairs of Russia. 2017. Part 1. P. 115–118 (in Russian).

[31] Averin A.I. Authentication of users by keyboard handwriting A.I. Averin, D.P. Sidorov. URL: http://cyberleninka.ru/article/n/autentifikatsiya–polzovatelya–po–klaviaturnomu–pocherku (accessed: 02.12.2019) (in Russian).

[32] Yandiev I.B. Study of temporal characteristics of keyboard handwriting for rapid authentication of personality I.B. Yandiev. Young scientist. 2017. № 14. P. 154–157 (in Russian).

Поступила в редакцию – 5 февраля 2020 г. Окончательный вариант – 25 мая 2020 г.
Received – February 05, 2020. The final version – May 25, 2020.