Обзорная статья

УДК 004.75:519.687.1+004.771

ББК 32.972.5

Д 58

doi: 10.53598/2410-3225-2021-2-281-72-81

**Организация безопасного удаленного доступа сотрудника
коммерческой компании, работающего вне офиса**
(Рецензирована)

**Виталий Анатольевич Довгаль¹, Сусана Касеевна Меретукова²,
Денис Игоревич Шередько³**

¹ Майкопский государственный технологический университет, Адыгейский государственный университет, Майкоп, Россия, urmia@mail.ru

^{2,3} Майкопский государственный технологический университет, Майкоп, Россия

² postforsusana@yandex.ru

³ sheredkoden@yandex.ru

Аннотация. Рассматриваются способы и особенности организации удаленного доступа сотрудниками коммерческой компании, выполняющими свои должностные обязанности, находясь вне офиса, что является актуальным в связи с необходимостью изоляции в условиях пандемии. Использование общедоступных каналов передачи данных требует применения эффективных систем безопасности информации. На основании рассмотрения угроз передачи данных, присущих удаленному доступу, и способов их нейтрализации в данной работе предлагаются варианты замены зарубежного программного обеспечения, используемого в российских коммерческих компаниях, аналогичным ему по реализуемым функциям отечественным в рамках тенденции импортозамещения.

Ключевые слова: информационная безопасность, безопасный удаленный доступ, угрозы информации при удаленном доступе, инфраструктура виртуальных рабочих столов, шлюз удаленных рабочих столов, виртуализация приложений

Review article

**Organization of secure remote access for an employee
of a commercial company working outside the office**

Vitaliy A. Dovgal¹, Susanna K. Meretukova², Denis I. Sheredko³

¹ Maikop State University of Technology, Adyghe State University, Maikop, Russia, urmia@mail.ru

^{2,3} Maikop State University of Technology, Maikop, Russia

² postforsusana@yandex.ru

³ sheredkoden@yandex.ru

Abstract. The article discusses the methods and features of organizing remote access by employees of a commercial company who perform their official duties while out of the office, which is relevant due to the need for isolation in a pandemic. The use of public data transmission channels requires the use of effective information security systems. Based on the consideration of data transmission threats inherent in remote access and ways to neutralize them, this paper suggests options for replacing foreign software used in Russian commercial companies with similar domestic functions in terms of the import substitution trend.

Keywords: information security, secure remote access, threats to information during remote access, virtual desktop infrastructure, remote desktop gateway, application virtualization

Введение

В настоящее время, особенно во время самоизоляции, вызванной пандемией коронавируса в 2020 г., выросла популярность работы из дома. По данным совместного аналитического доклада ВЦИОМ и Social Business Group, доля россиян, работающих удаленно, во время режима самоизоляции из-за коронавируса возросла в восемь раз [1]. Но даже после снижения уровня заболевших удаленная работа остается востребованной. В июне 2020 г. количество объявлений с предложением дистанционной работы выросло на 14% по сравнению с маем, а в июле – еще на 14% по сравнению с июнем [2]. Удаленная работа имеет свои преимущества по сравнению с работой непосредственно в офисе: работнику не нужно тратить время на дорогу, он может трудоустроиться у работодателя, находящегося в одном регионе, физически находясь при этом в другом, снижаются расходы сотрудника на транспорт и питание. На законодательном уровне удаленная работа в России регулируется федеральным законом «О внесении изменений в Трудовой кодекс Российской Федерации в части регулирования дистанционной (удаленной) работы и временного перевода работника на дистанционную (удаленную) работу по инициативе работодателя в исключительных случаях», принятого в 2020 году [3].

В процессе выполнения должностных обязанностей с использованием удаленной работы есть необходимость организовывать удаленный доступ к определенным ресурсам организации. В настоящей статье рассмотрены риски информационной безопасности, возникающие при удаленном доступе сотрудника к рабочему столу компьютера, установленного в офисе коммерческой компании, а также представлены способы минимизации указанных рисков на основе использования отечественных программных продуктов.

1. Исследование способов обеспечения безопасности удаленного доступа

Удаленная работа – это способ взаимодействия сотрудников, когда они находятся не в офисе и выполняют свою работу. Основные виды удаленной работы следующие [4]:

- дистанционная работа на постоянной основе;
- временная дистанционная работа;
- периодическая дистанционная работа;
- дистанционная работа в исключительных случаях.

При выполнении сотрудником, находящимся на удаленной работе, своих должностных обязанностей появляется необходимость организовывать удаленный доступ к определенным вычислительным ресурсам организации. Для осуществления удаленного доступа можно использовать один из способов:

1. подключение к определенному компьютеру, расположенному в организации;
2. использование инфраструктуры виртуальных рабочих столов [5];
3. использование виртуализации приложений [5].

Первый способ предполагает подключение сотрудника к определенному компьютеру в сети организации. Схема подключения устройств показана на рисунке 1 [6].

Достоинства данного способа [7]:

- доступ сотрудника к компьютеру организации в командировке;
- замену уволившемуся сотруднику можно найти в другом регионе;
- не высокие затраты на переход от очного формата работы к удаленному;
- быстрая смена очного формата работы сотрудника дистанционным.

Недостаток данного способа: требование отдельного компьютера для каждого сотрудника.

Рис. 1. Схема подключения сотрудников к компьютерам, расположенным в сети организации

Второй способ, называемый инфраструктурой виртуальных рабочих столов (*англ.* Virtual Desktop Infrastructure, VDI), является технологией, позволяющей создавать виртуальную ИТ-инфраструктуру и разворачивать полноценные рабочие места на базе одного или нескольких серверов, на которых работает множество виртуальных машин [8]. То есть сотрудник подключается не к отдельному компьютеру, а к специальному серверу, на котором находятся операционные системы (ОС), одну из которых и использует подключающийся сотрудник. Пользователи получают доступ к личному виртуальному рабочему столу или к нескольким рабочим столам, настроенным одинаковым образом [5].

Схема виртуального рабочего стола показана на рисунке 2 [9].

Рис. 2. Схема инфраструктуры виртуальных рабочих столов

Достоинства инфраструктуры виртуальных рабочих столов:

- гибкое администрирование ИТ-инфраструктурой [10];
- мониторинг всех компонентов среды [10];
- наличие технологии моментальных снимков, с помощью которой пользователи могут вернуться к ранее сохраненному стабильному состоянию ОС, например, в случае заражения вредоносным программным обеспечением (ПО) [11];
- простое масштабирование [12].

Недостатки данной инфраструктуры [12]:

- большие финансовые затраты на развертывание VDI;
- зависимость от сетевой инфраструктуры компании (VDI не будет

демонстрировать свои преимущества при невысокой пропускной способности сети офиса);

- большие временные затраты при внедрении в крупных компаниях (организация VDI на 1000 рабочих мест и больше может занять от нескольких месяцев до года).

Третий способ удаленного доступа – виртуализация приложений – позволяет использовать приложения, установленные на сервере, так, как будто бы они установлены на рабочем компьютере сотрудника [13]. Пример такой платформы – Microsoft Application Virtualization (App-V), разработанная компанией Microsoft [14].

Схема устройства виртуализации приложений, на примере App-V, показана на рисунке 3 [15].

Рис. 3. Схема устройства виртуализации приложений

Достоинства использования приложений на сервере [13]:

- централизованное управление приложениями;
- простота обновления и исправления приложений;
- меньший расход ресурсов по сравнению с виртуальной ОС;
- простота контроля использования лицензий.

Недостаток схемы: любой человек, имеющий физический доступ к серверу App-V, потенциально может атаковать всю клиентскую базу. Серверы App-V должны храниться в физической защищенной серверной комнате с контролируемым доступом [16].

Один из наиболее часто используемых способов удаленного доступа – это подключение одного сотрудника к одному компьютеру, расположенному в организации. Именно этот способ и будет подробно рассмотрен в настоящей статье.

2. Угрозы, присущие удаленному доступу к определенному компьютеру, и способы их нейтрализации

Для выбранного вида удаленного доступа типичными информационными угрозами являются [6, 17, 18]:

- атака «человек посередине»;
- анализ сетевого трафика («перехват»);
- подмена субъекта или объекта сети (так называемый «маскарад»);
- атака «грубой силы» (*англ.* brute force);
- вредоносные программы;
- отказ в обслуживании (Deny of Service, DoS), или «распределенный» отказ в обслуживании (Distributed Deny of Service, DDoS);
- хакерство;
- крекинг – акт проникновения в компьютерную систему или сеть;
- уязвимости приложений (например, ошибки безопасности памяти или ошибочные проверки подлинности, которые может содержать программное обеспечение);

- человеческий фактор;
- кража устройств и носителей конфиденциальной информации.

Для каждой из указанных угроз существуют свои способы нейтрализации. Например, для защиты от таких угроз, как атака «человек посередине», анализ сетевого трафика («перехват») и хакерство нужно применять шифрование [19]. Его можно реализовать с помощью виртуальной частной сети (*англ.* Virtual Private Network или VPN). При должном уровне реализации и использовании специального программного обеспечения виртуальная частная сеть сможет обеспечить высокий уровень шифрования передаваемой информации.

VPN использует несколько популярных протоколов [20]: туннельный протокол типа точка-точка (Point-to-Point Tunneling Protocol, PPTP), протокол туннелирования второго уровня (Layer 2 Tunneling Protocol, L2TP), специально разработанный для создания безопасных соединений Internet Protocol Security (IPSec), Secure Sockets Layer (SSL) и Transport Layer Security (TLS) (с их популярными реализациями Microsoft SSTP (SSL 3.0) и Open VPN (SSL 3.0/TLS 1.2)). Каждый из перечисленных протоколов имеет свои достоинства и недостатки, которые определяют уязвимости, присутствующие у виртуальных частных сетей (например, возможность определения реального публичного IP-адреса устройства, работающего через VPN, или периодический разрыв VPN-подключения и, как следствие, внезапный выход трафика в публичную сеть) [9]. Кроме того, не всегда DNS-запросы уходят внутрь виртуальной сети и там обрабатываются собственными DNS-серверами. На практике при установке подключения не всегда прописываются доверенные серверы (например, Google Public DNS или Open DNS) – часто используются DNS-серверы, выданные публичной сетью, ответ от которых может быть некорректным, и вместо реального адреса запрашиваемого домена пользователь может получить поддельный. Побочный эффект от данной проблемы – угроза анонимности, то есть злоумышленник может выяснить адреса DNS-серверов пользователя и таким образом получить информацию о его Интернет-провайдере и примерном местоположении.

Для минимизации угрозы от атак «грубой силы» можно использовать следующие средства: сложные пароли, многофакторную аутентификацию и ограничение попыток ввода пароля [21]. А для защиты от вирусного программного обеспечения необходимо использовать антивирусные программы, которые также могут нейтрализовать такие угрозы, как хакерство и крекинг [22].

Для нейтрализации вышеперечисленных угроз используется следующее оборудование – межсетевые экраны, маршрутизаторы, системы обнаружения и предотвращения вторжений, аппаратные модули доверенной загрузки и смарт-карты.

В настоящее время в условиях санкций, налагаемых импортными производителями программного обеспечения, имеет большое значение для организации удаленного доступа сотрудников, находящихся вне офиса, использовать отечественное программное обеспечение.

3. Обеспечение безопасного удаленного доступа для коммерческой компании

Для удаленного подключения сотрудников к рабочему столу компьютера, расположенного в офисе компании, используются различные программы и сервисы. Из отечественных программ можно назвать RMS Удаленный доступ [23], состоящую из следующих основных частей: модуля управления («Клиент») и удаленного модуля («Хост»). Программный продукт поддерживает несколько способов авторизации: с использованием пароля, с использованием логина и пароля, с помощью учетной записи в Windows и авторизация через сервер. Программа обладает рядом отличительных осо-

бенностей и достоинств, с которыми можно ознакомиться на сайте разработчика.

Другим примером отечественного ПО для удаленного доступа является программный комплекс АССИСТЕНТ [24]. Отличительной особенностью программы является то, что встроенное средство защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, прошло сертификационные испытания по 4 уровню доверия. Данное средство поставляется только при использовании лицензии «Корпорация + ФСТЭК». Оно позволяет применять ПО в государственных информационных системах до 1 класса защищенности (включительно), информационных системах персональных данных до 1 уровня защищенности (включительно), автоматизированных системах управления до 1 класса защищенности (включительно), на объектах критической информационной инфраструктуры до 1 категории (включительно) [25]. Наличие большого количества лицензий ПО АССИСТЕНТ позволяет использовать его как в малых компаниях, так и в крупных. А лицензии «Корпорация+» и «Корпорация + ФСТЭК» позволяют использовать собственные управляющие серверы [24].

Для создания VPN одним из рекомендуемых отечественных решений можно использовать продукты сетевой безопасности семейства «ЗАСТАВА» [26]. Для организации VPN требуются программный комплекс «ЗАСТАВА-Офис» и ПО «ЗАСТАВА-Клиент», являющиеся межсетевыми экранами и VPN-агентами. Первый из комплексов может реализовывать функции прикладного проксирования популярных сетевых сервисов и протоколов (Telnet, FTP, SMTP, HTTP, SOCKS), а также маскирование топологии защищаемой сети в режиме VPN-туннелирования либо с использованием встроенного централизованно управляемого NAT-сервера [27]. «ЗАСТАВА-Офис» получил сертификаты соответствия ФСБ к шифровальным средствам по классу КС1, КС2 и КС3. В свою очередь «ЗАСТАВА-Клиент» на отдельных рабочих станциях и устройствах мобильных пользователей обеспечивает полный набор функций сетевой защиты (например, при работе в сети Интернет, включая режим выделения мобильному пользователю внутреннего локального адреса для удаленного VPN-доступа в защищенную корпоративную сеть). «ЗАСТАВА-Офис» позволяет обеспечить VPN по уровню КС1 и КС2, а также имеет сертификат ФСТЭК.

Кроме того, можно подключить систему централизованного управления «ЗАСТАВА-Управление», позволяющую создавать единую политику безопасности – набор правил для защищаемой сети [28]. Данное ПО получило как сертификаты соответствия ФСБ к шифровальным средствам по классу КС1, КС2 и КС3, которые находятся на продлении, так и действующий сертификат ФСТЭК.

Другим примером отечественного средства для создания виртуальной частной сети является КриптоПро NGate [29]. Указанный продукт сертифицирован по требованиям, предъявляемым к СКЗИ, и использует российские криптографические алгоритмы. Компоненты решения сертифицированы ФСБ России по классам КС1, КС2, КС3 и используют в своем составе сертифицированное СКЗИ КриптоПро CSP с российскими криптографическими алгоритмами ГОСТ 28147-89, ГОСТ Р 34.11-94/ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2001/ГОСТ Р 34.10-2012. С помощью динамического VPN-туннеля шлюза комплекс NGate обеспечивает доступ сотрудника к удаленной сети по любым протоколам и портам внутри туннеля.

Заключение

В данном исследовании рассмотрена возможность применения отечественного программного обеспечения для организации удаленного доступа в крупной коммерческой компании. Сравнивая описываемые в статье решения российских производителей, можно сделать вывод, что наиболее оптимальным для использования являются – АС-

СИСТЕНТ с версией лицензии «Корпорация + ФСТЭК» и продукты семейства «ЗАСТАВА». Выбор первого из перечисленных программных решений обоснован следующими причинами:

- программный комплекс АССИСТЕНТ поддерживает большее количество ОС
- даже уже имеются сертификаты совместимости для различных версий Linux (в RMS совместимость с Linux еще тестируется);
- комплекс обладает встроенным сертифицированным средством защиты от несанкционированного доступа;
- в комплексе есть возможность использования сессионных паролей.

Программный комплекс АССИСТЕНТ необходимо установить как на устройство сотрудника, с которого он будет подключаться, так и на удаленный компьютер. Также необходима установка серверной части данного ПО.

Выбор продуктов семейства «ЗАСТАВА» обосновывается наличием сертификата совместимости с ранее выбранным комплексом АССИСТЕНТ. Решение необходимо установить на устройства сотрудника и на VPN-сервер.

Список литературы:

1. ВЦИОМ. Число работающих удаленно россиян во время пандемии возросло в восемь раз // Информационное агентство ТАСС. URL: <https://tass.ru/ekonomika/8478435> (дата обращения: 03.05.2021).
2. Власова И. Без отдыха и опозданий: почему увеличился запрос на удаленку // Информационное агентство «Газета.Ру». URL: <https://www.gazeta.ru/business/2020/08/25/13211443.shtml> (дата обращения: 03.05.2021).
3. О внесении изменений в Трудовой кодекс Российской Федерации в части регулирования дистанционной (удаленной) работы и временного перевода работника на дистанционную (удаленную) работу по инициативе работодателя в исключительных случаях: Федеральный закон от 8 декабря 2020 г. N 407-ФЗ // Собрание законодательства РФ. 2020. № 50. Ст. 8052.
4. Новые виды удаленной работы по ТК РФ // Web-сайт «Кадровое дело». URL: <https://www.kdelo.ru/art/386028-vidy-udalennoy-raboty-po-tk-rf-21-m1> (дата обращения: 03.05.2021).
5. Савельев А. Remote Desktop виртуализация // Национальный Открытый Университет «ИНТУИТ». URL: <https://intuit.ru/studies/courses/2324/624/lecture/13610> (дата обращения: 03.05.2021).
6. Серебrenникова Е. Защита RDP подключений с помощью RD Gateway и КриптоПро CSP // База знаний компании «Криптопро». URL: <https://support.cryptopro.ru/index.php?Knowledgebase/Article/View/292/0/zshhit-rdppodkljuchenijj-s-pomoshhju-rdgateway-i-kriptopro-csp> (дата обращения: 04.05.2021).
7. Как выбрать самый удобный способ доступа к 1С в облаке? // Web-сайт «42Clouds». URL: <https://42clouds.com/ru-ru/articles/1c-v-oblake-rdp-remoteapp-web-dostup-vyberaem-vmeste.html> (дата обращения: 04.05.2021).
8. Глоссарий // Документация TIONIX. URL: <https://docs.tionix.ru/2.8.17/glossary/index.html#term-vdi-virtual-desktop-infrastructure> (дата обращения: 04.05.2021).
9. VMware View-Virtual Desktop Infrastructure – VDI // Российский Интернет-портал и аналитическое агентство «Tadviser». URL: https://www.tadviser.ru/index.php/Продукт:VMware_View_-_Virtual_Desktop_Infrastructure_-_VDI?cache=no&ptype=integr (дата обращения: 04.05.2021).
10. TIONIXVDI // Web-сайт «TIONIX». URL: <https://tionix.ru/services/tionix-vdi/> (дата обращения: 04.05.2021).
11. VDI и RDS: какая между ними разница и в чем преимущества // Web-сайт компании «ИБИК». URL: <https://www.ibik.ru/ru/vdi-vs-rds-difference-between-vdi-rdp/> (дата обращения: 04.05.2021).

12. VDI: как работает, плюсы, минусы и кому подходит // Блог компании “Selectel”. URL: <https://selectel.ru/blog/vdi-technology-review/> (дата обращения: 04.05.2021).
13. Савельев А. App-V // Национальный Открытый Университет «ИНТУИТ». URL: <https://intuit.ru/studies/courses/2324/624/lecture/13607> (дата обращения: 04.05.2021).
14. Начало работы с App-V для Windows 10 // Документация Майкрософт. URL: <https://docs.microsoft.com/ru-ru/windows/application-management/app-v/appv-getting-started> (дата обращения: 04.05.2021).
15. Microsoft Application Virtualization // Web-сайт “Enterprise IT Management”. URL: <https://statemigration.com/microsoft-application-virtualization/> (дата обращения: 04.05.2021).
16. Соображения безопасности, связанные с App-V // Документация Майкрософт. URL: <https://docs.microsoft.com/ru-ru/windows/application-management/app-v/appv-security-considerations> (дата обращения: 04.05.2021).
17. Хорев П.Б. Программно-аппаратная защита информации. Москва: ИНФРА-М, 2021. 327 с. URL: <https://znanium.com/read?id=365036> (дата обращения: 05.05.2021).
18. Джост М., Кобб М. Угрозы безопасности в интернете // Национальный Открытый Университет «ИНТУИТ». URL: <https://intuit.ru/studies/courses/18038/122/lecture/3517> (дата обращения: 05.05.2021).
19. Довгаль В.А., Довгаль Д.В. Анализ безопасности роя дронов, противостоящего атакам злоумышленников // Дистанционные образовательные технологии: сб. трудов V Междунар. науч. конф. Симферополь, 2020. С. 372–377.
20. Какие существуют разновидности VPN и чем они отличаются // Блог Касперского. URL: <https://www.kaspersky.ru/blog/vpn-implementations/11156/> (дата обращения: 05.05.2021).
21. Миллс М. Атака грубой силы: что это такое и как эта атака помогает взломать пароли // Web-сайт “ITIGIC”. URL: <https://itigic.com/ru/brute-force-attack-what-it-is-and-how-this-attack-works/> (дата обращения: 05.05.2021).
22. Сычев Ю.Н. Защита информации и информационная безопасность. Москва: ИНФРА-М, 2021. 201 с. URL: <https://znanium.com/read?id=365029> (дата обращения: 05.05.2021).
23. RMS Удаленный доступ // Веб-сайт продукта «RMS Удаленный доступ». URL: <https://rmansys.ru/> (дата обращения: 06.05.2021).
24. АССИСТЕНТ // Веб-сайт продукта «АССИСТЕНТ». URL: <https://мойассистент.рф/> (дата обращения: 06.05.2021).
25. Сертификаты // Веб-сайт продукта «АССИСТЕНТ». URL: <https://мойассистент.рф/сертификаты> (дата обращения: 06.05.2021).
26. Продукт сетевой безопасности «ЗАСТАВА». URL: <https://zastava.ru/> (дата обращения: 06.05.2021).
27. Семейство продуктов «ЗАСТАВА». URL: <https://docplayer.ru/26842370-2-semeystvo-produktov-zastava-5-3.html> (дата обращения: 06.05.2021).
28. ЦУП «ЗАСТАВА-Управление» // Веб-сайт семейства продуктов «ЗАСТАВА». URL: <https://zastava.ru/zastava/the-gate-control/> (дата обращения: 06.05.2021).
29. КриптоПро NGate // Веб-сайт компании «КриптоПро». URL: <https://cryptopro.ru/products/ngate> (дата обращения: 06.05.2021).

References:

1. VTsIOM. The number of Russians working remotely during the pandemic increased eight-fold // TASS Information Agency. URL: <https://tass.ru/ekonomika/8478435> (date of access: 03.05.2021).
2. Vlasova I. Without rest and delays: why the request for remote control has increased // Gazeta.Ru Information Agency. URL: <https://www.gazeta.ru/business/2020/08/25/13211443.shtml> (date of access: 03.05.2021).
3. On amendments to the Labor Code of the Russian Federation regarding the regulation of distant (remote) work and temporary switch of an employee to distant (remote) work at the initiative of the employer in exceptional cases: Federal Law of December 8, 2020 N 407-FZ // Collection of legislation of the Russian Federation. 2020. No. 50. Art. 8052.
4. New types of remote work according to the Labor Code of the Russian Federation // “Per-

sonnel business” Web-site. URL: <https://www.kdelo.ru/art/386028-vidy-udalennoy-raboty-po-tk-rf-21-m1> (date of access: 03.05.2021).

5. Savelyev A. Remote Desktop virtualization // National Open University of “INTUIT”. URL: <https://intuit.ru/studies/courses/2324/624/lecture/13610> (date of access: 03.05.2021).

6. Serebrennikova E. Protection of RDP connections using RD Gateway and CryptoPro CSP // Knowledge base of the Cryptopro company. URL: <https://support.cryptopro.ru/index.php?Knowledgebase/Article/View/292/0/zshhit-rdppodkljuchenijj-s-pomoshhju-rdgateway-i-kriptopro-csp> (date of access: 04.05.2021).

7. How to choose the most convenient way to access 1C in the cloud? // The 42Clouds Web Site. URL: <https://42clouds.com/ru-ru/articles/1c-v-oblake-rdp-remoteapp-web-dostup-vyberaem-vmeste.html> (date of access: 04.05.2021).

8. Glossary // TIONIX documentation. URL: <https://docs.tionix.ru/2.8.17/glossary/index.html#term-vdi-virtual-desktop-infrastructure> (date of access: 04.05.2021).

9. VMware View-Virtual Desktop Infrastructure – VDI // Russian Internet portal and TAdviser analytical agency. URL: https://www.tadviser.ru/index.php/Product:VMware_View_-_Virtual_Desktop_Infrastructure_-_VDI?cache=no&type=integr (date of access: 04.05.2021).

10. TIONIXVDI // Web-сайт “TIONIX”. URL: <https://tionix.ru/services/tionix-vdi/> (date of access: 04.05.2021).

11. VDI and RDS: what is the difference between them and what are the advantages // Web site of the “IBIK” company. URL: <https://www.ibik.ru/ru/vdi-vs-rds-difference-between-vdi-rdp/> (date of access: 05/04/2021).

12. VDI: how it works, pros, cons and who suits them // Blog of the Selectel company. URL: <https://selectel.ru/blog/vdi-technology-review/> (date of access: 04/05/2021).

13. Saveliev A. App-V // National Open University “INTUIT”. URL: <https://intuit.ru/studies/courses/2324/624/lecture/13607> (date of access: 05/04/2021).

14. Getting Started with App-V for Windows 10 // Microsoft Documentation. URL: <https://docs.microsoft.com/ru-ru/windows/application-management/app-v/appv-getting-started> (date of access: 05/04/2021).

15. Microsoft Application Virtualization // Web-сайт “Enterprise IT Management”. URL: <https://statemigration.com/microsoft-application-virtualization/> (date of access: 04.05.2021).

16. Security Considerations Related to App-V // Microsoft documentation. URL: <https://docs.microsoft.com/ru-ru/windows/application-management/app-v/appv-security-considerations> (date of access: 04.05.2021).

17. Khorev P.B. Hardware and software information protection. Moscow: INFRA-M, 2021. 327 p. URL: <https://znanium.com/read?id=365036> (date of access: 05.05.2021).

18. Jost M., Cobb M. Internet security threats // National Open University of “INTUIT”. URL: <https://intuit.ru/studies/courses/18038/122/lecture/3517> (date of access: 05.05.2021).

19. Dovgal V.A., Dovgal D.V. Analysis of the security of a swarm of drones resisting attacks by intruders // Distance educational technologies: collection of proceedings of the 5th International scient. conf. Simferopol, 2020. P. 372–377.

20. What types of VPN exist and how they differ // Kaspersky's blog. URL: <https://www.kaspersky.ru/blog/vpn-implementations/11156/> (date of access: 05.05.2021).

21. Mills M. Brute force attack: what it is and how this attack helps to crack passwords // Website of “ITIGIC”. URL: <https://itigic.com/ru/brute-force-attack-what-it-is-and-how-this-attack-works/> (date of access: 05.05.2021).

22. Sychev Yu.N. Information protection and information security. Moscow: INFRA-M, 2021. 201 p. URL: <https://znanium.com/read?id=365029> (date of access: 05.05.2021).

23. RMS Remote access // RMS Remote Access product website. URL: <https://rmansys.ru/> (date of access: 06.05.2021).

24. ASSISTANT // Website of “ASSISTANT” product. URL: <https://myassistant.rf/> (date of access: 06.05.2021).

25. Certificates // Website of “ASSISTANT” product. URL: <https://myassistant.rf/Certificates> (date of access: 06.05.2021).

26. “ZASTAVA” product of network security URL: <https://zastava.ru/> (date of access:

06.05.2021).

27. Family of “ZASTAVA” products. URL: <https://docplayer.ru/26842370-2-semeystvo-produktov-zastava-5-3.html> (date of access: 06.05.2021).

28. “ZASTAVA-Management” TsUP // Website of the family of “ZASTAVA” products. URL: <https://zastava.ru/zastava/the-gate-control/> (date of access: 06.05.2021).

29. CryptoPro NGate // Website of the CryptoPro company. URL: <https://cryptopro.ru/products/ngate> (date of access: 06.05.2021).

Авторы заявляют об отсутствии конфликта интересов.

The authors declare no conflicts of interests.

Статья поступила в редакцию 16.05.2021; одобрена после рецензирования 18.06.2021; принята к публикации 20.06.2021.

The article was submitted 16.05.2021; approved after reviewing 18.06.2021; accepted for publication 20.06.2021.

© В.А. Довгаль, С.К. Меретукова, Д.И. Шередько, 2021