ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

DOI: 10.6060/ivecofin.2021493.558
УДК: 004.056.5

ОЦЕНКА СТОИМОСТИ ПРИОБРЕТЕНИЯ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В СФЕРЕ ЗДРАВООХРАНЕНИЯ

Е.Д. Родионычева, А.С. Голубев

Екатерина Дмитриевна Родионычева* (ORCID 0000-0002-3986-1065), Александр Сергеевич Голубев (ORCID 0000-0003-2573-242X)
Ивановский государственный университет, ул. Ермака, 39, Иваново, 153025, Россия
E-mail: rodionycheva.97@yandex.ru*, golubewalex@bk.ru

В статье рассмотрен и проанализирован рынок программно-аппаратных комплексов, обеспечивающих необходимый уровень информационной безопасности и имеющих необходимые сертификаты ФСТЭК и ФСБ, которые могут быть использованы в государственных информационных системах сферы здравоохранения. Поскольку в настоящее время отмечается тенденция централизации информационных систем в сфере здравоохранения на уровне региона, то в связи с этим, рост требований к оборудованию, обеспечивающему защиту данных, стремительно увеличивается. Защита персональных данных является неотъемлемой частью внедряемой системы, этому аспекту должно уделяться внимание на всех этапах жизненного цикла системы: от ее проектирования до внедрения и сопровождения. Отмечается, что наиболее надежным с точки зрения безопасности является подход, подразумевающий проверку прав доступа пользователей на уровне базы данных. Для этого применяются встроенные средства контроля доступа, в основе которых лежит комбинация дискреционной и ролевой моделей безопасности. В статье представлена модель виртуализации с дифференциацией на уровни, рассмотрен каждый из них с выделением требований и особенностей. Проведен сравнительный анализ отечественного рынка программно-аппаратных комплексов обеспечения информационной безопасности по ряду характеристик, в том числе, стоимости оборудования. На основе объективного анализа сформированы выводы и заключения, касающиеся отечественного оборудования. Данный материал может быть полезен в ключе обеспечения информационной безопасности при внедрении региональных медицинских информационных систем.

Ключевые слова: информационная безопасность, программно-аппаратный комплекс, государственные информационные системы, медицинские информационные системы, защита персональных данных.

ASSESSMENT OF THE COST OF PURCHASING A SOFTWARE AND HARDWARE COMPLEX TO ENSURE INFORMATION SECURITY OF INFORMATION SYSTEMS IN THE HEALTHCARE

E.D. Rodionycheva, A.S.Golubev

Ekaterina D. Rodionycheva* (ORCID 0000-0002-3986-1065), Alexander S. Golubev (ORCID 0000-0003-2573-242X)
Ivanovo State University, st. Ermaka, 39, Ivanovo, 153025, Russia
E-mail: rodionycheva.97@yandex.ru*, golubewalex@bk.ru

The article considers and analyzes the market of software and hardware systems that provide the necessary level of information security and have the necessary FSTEC and FSB certificates, which can be used in state information systems in the healthcare sector. Since there is currently a tendency to centralize information systems in the healthcare sector at the regional level, in this regard, the growth in requirements for equipment that ensures data protection is rapidly increasing. Personal data protection is an integral part

of the system being implemented; attention should be paid to this aspect at all stages of the system life cycle: from its design to implementation and maintenance. It is noted that the most reliable from a security point of view is the approach that involves checking user access rights at the database level. It uses built-in access controls based on a combination of discretionary and role-based security models. The article presents a virtualization model with differentiation into levels, each of them is considered, highlighting requirements and features. A comparative analysis of the domestic market of software and hardware systems for information security has been carried out for a number of characteristics, including the cost of equipment. On the basis of an objective analysis, conclusions and conclusions regarding domestic equipment were formed. This material can be useful in terms of ensuring information security in the implementation of regional medical information systems.

Keywords: information security, software and hardware complex, state information systems, medical information systems, personal data protection.

Для цитирования:
Родионычева Е.Д., Голубев А.С. Оценка стоимости приобретения программно-аппаратного комплекса для обеспечения информационной безопасности информационных систем в сфере здравоохранения. *Известия высших учебных заведений. Серия «Экономика, финансы и управление производством» [Ивэкофин]*. 2021. № 03(49). С.124-129. DOI: 10.6060/ivecofin.2021493.558

For citation:
Rodionycheva E.D., Golubev A.S. Assessment of the cost of purchasing a software and hardware complex to ensure information security of information systems in the healthcare. *Ivecofin.* 2021. № 03(49). С.124-129. DOI: 10.6060/ivecofin.2021493.558 (in Russian)

ВВЕДЕНИЕ

В настоящее время, в рамках Национального проекта «Здравоохранение», внедрение медицинской информационной системы (МИС) – это необходимость исполнения требований государства, и ее выбор регламентируется нормативно-правовыми актами Департаментов здравоохранения субъектов Российской Федерации.

Информация, обрабатываемая в МИС, включает в себя персональные данные пациентов, представляющие собой медицинскую тайну. Следовательно, доступ к такой информации должен быть ограничен и строго контролироваться.

Следует отметить, что государство предъявляет серьезные требования к безопасности персональных данных граждан, поэтому, каждая внедряемая система проходит жесткий контроль. Программное обеспечение должно соответствовать требованиям по защите информации, что подтверждается сертификатами, выданными ФСТЭК России и ФСБ России.

Сертификация ФСБ предназначена для проверки подсистем ПО, использующих криптографическую защиту. Для ознакомления с требованиями систем сертификации ФСБ необходимо наличие специальных допусков, поскольку они не являются публичными и в свободном доступе их не найти.

Прохождение сертификации ФСТЭК необходимо для проверки соответствия требованиям технической защиты информации некрипто-графическими методами. В частности, проводятся проверки:

– на соответствие требованиям, связанным с защитой от неразрешенного доступа к информации;
– на соответствие требованиям Технических условий;
– на отсутствие возможностей, которые не указаны в документации, и связанные с безопасностью информации будущего пользователя;
– исследование датчиков случайных чисел на соответствие криптографическим требованиям и др.

Наиболее надежным с точки зрения безопасности является подход, подразумевающий проверку прав доступа пользователей на уровне базы данных (БД). Для этого применяются встроенные средства контроля доступа, в основе которых лежит комбинация дискреционной и ролевой моделей безопасности. Где в качестве защищаемых объектов выступают объекты БД (таблицы, представления и т.д.), в качестве субъектов безопасности – пользователи или группы пользователей МИС, а для каждой пары «субъект безопасности – защищаемый объект» задается список разрешенных операций: вставка, выборка, редактирование, удаление.

АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

В настоящее время ситуация с внедрением МИС от региона к региону отличается. Поскольку активная информатизация здравоохранения в регионах началась задолго до утверждения Минздравом требований к государственным информационным системам в сфере здравоохранения [1] медицинские организации могли внедрять как локаль-

ную, независимую от других медицинских организаций МИС, так единую МИС на весь регион. Каждая отдельная медицинская организация сама принимала решение по выбору МИС, ее архитектурных и функциональных возможностей.

Сейчас во время этапа развития цифрового здравоохранения, рассчитанного на 2019–2024 гг., для многих регионов становится актуальным вопрос объединения различных МИС или их замены на единую региональную МИС.

В первом случае этого возможно добиться посредством интеграционной шины для объединения нескольких локальных МИС между собой. Но использование интеграционного подхода является недостатком относительно информационной безопасности (ИБ). Разные МИС реализуют разные уровни информационной безопасности, в связи с этим возможна утечка персональных данных из баз данных МИС. Кроме того, к заражению компьютеров и серверов с информацией о пациентах и утечке персональных данных способствует несоответствие локальной сети медицинской организации требованиям ИБ и отсутствие антивирусной защиты.

Региональные центры обработки данных (ЦОД), в которых разворачиваются централизованные решения, напротив защищены сертифицированными средствами защиты информации и в обязательном порядке проходят аттестацию по требованиям безопасности информации, что гарантирует сохранность персональных данных пациентов. Регулируется и отслеживается доступ сотрудников к оборудованию, настроено резервирование данных и обеспечена возможность непрерывной работы в случае инцидентов с потерей электроэнергии.

Согласно «Методическим рекомендациям по обеспечению функциональных возможностей медицинских информационных систем медицинских организаций (МИС МО)» одним из основных требований к МИС является обеспечение отказоустойчивости за счет распределения нагрузки и резервирования [2]. Данную задачу можно выполнить при помощи виртуализации, которая представляет собой предоставление набора вычислительных ресурсов или их логического объединения, абстрагированного от аппаратной реализации, и обеспечивающего при этом логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе [3]. Относительно развертывания МИС речь пойдет не просто о сервере виртуализации, а о целом виртуальном центре обработки данных (ВЦОД).

Модель ВЦОД можно представить в виде схемы представленной на рис. 1. На каждом уровне ресурсы объединяются в пулы для последующего использования гипервизором согласно настройкам администратора.

На первом уровне виртуализации расположена сеть. Она обеспечивает взаимосвязь всех устройств.

На втором уровне – виртуализация систем хранения данных, которая создает пул доступных для использования хранилищ данных.

Далее следует виртуализация вычислительных ресурсов. Виртуальная машина может использовать часть или все ядра одного многоядерного процессора, настройка может происходить по требованиям системы и при необходимости масштабирования системы.

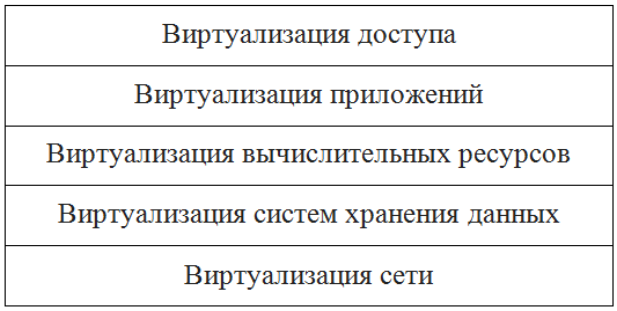

Рисунок. 1 Модель ВЦОД
Figure 1. Virtual data center model

На четвертом уровне располагается виртуализация приложений, которая позволяет эффективно работать со всеми инструментами без привязки к операционным системам. Поскольку требования к МО – использовать только ПО, внесенное в реестр российских программ для электронных вычислительных машин и баз данных, то важна поддержка и возможность работы с операционными системами семейства Linux.

На высшем уровне расположена виртуализация доступа. Она отвечает за эффективность служб аутентификации.

Основополагающей частью является гипервизор, с его помощью можно распределять в нужном объеме физические ресурсы для каждого виртуального сервера. Это позволит, в рамках одно физического сервера, развернуть несколько виртуальных серверов, каждый из которых будет задействован в работе разных подсистем МИС и отвечать за разные функции. В свою очередь, это оптимизирует потребление вычислительных ресурсов и ресурсов хранения, которые необходимы для эффективной работы и изоляции процессов.

Сервера должны быть объединены в отказоустойчивый кластер из физических серверов. В случае отказа одного сервера не приведет к пол-

ной неработоспособности всего кластера, а его задачи распределятся между другими серверами в автоматическом режиме.

Поскольку, для подключения медицинских организаций к ЦОД используются каналы связи, предоставляемые провайдерами, необходимость обеспечения целостности и конфиденциальности передаваемых данных по ним требует использования криптографических шлюзов – аппаратно-программных комплексов, работающих на основе технологии VPN и обеспечивающих «прозрачное» шифрование информационных сетевых потоков между объектами, отдаленными друг от друга. При этом в ЦОД может использоваться различное адресное пространство, а взаимосвязь серверов и объектов сети производится посредством маршрутизации данных. В таких случаях для построения защиты каналов связи используются разработанные технологии VPN: IPsec, SSL VPN, ViPNet VPN.

Реализация функций криптографической защиты информации должна соответствовать Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3 и соответствовать следующим профилям защиты [4]:

– «Профиль защиты межсетевых экранов типа А четвертого класса защиты ИТ.МЭ.А4.ПЗ»;

– «Профиль защиты межсетевых экранов типа Б четвертого класса защиты ИТ.МЭ.Б4.ПЗ»;

– «Профиль защиты межсетевых экранов типа В четвертого класса защиты ИТ.МЭ.В4.ПЗ»;

– «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты ИТ.СОВ.С4.ПЗ».

Рассмотрим российский рынок программно-аппаратных комплексов входящих в реестр отечественного ПО, форм-фактора 1U. Сравнение оборудования приведено в табл. 1.

Таблица 1. Сравнительный анализ моделей программно-аппаратных комплексов
Table 1. Comparative analysis of models of software and hardware complex

Модель	ViPNet Coordinator HW1000	ViPNet Coordinator HW2000	ViPNet Coordinator HW5000	Diamond VPN/FW 4101	Diamond VPN/FW 4105	Diamond VPN/FW 4106	ALTELL NEO 310
Пропускная способность VPN, Гбит/с	до 0,95	до 2,7	до 5,5	до 1,8	до 2,2	до 2,7	до 15,5
Пропускная способность L2 VPN, Гбит/с	до 0,8	до 2,4	до 4,5	до 0,4	до 0,9	до 0,9	до 13,5
Рекомендуемое число VPN-клиентов	до 1000	до 5000	до 6000	до 1000	до 1000	до 1000	до 1000
Сетевые интерфейсы (медные) 1 Гбит/с, шт.	Q4, Q6 - 4x RJ45 Q5 - 6x RJ45 1 Гбит/с	4x RJ45 1 Гбит/с	4x RJ45 1 Гбит/с	8xRJ45 1 Гбит/с	8xRJ45 1 Гбит/с	8xRJ45 1 Гбит/с	8×RJ45 Гбит/с
Сетевые интерфейсы (оптические), шт.	Q6 - 2x SFP 1 Гбит/с	4x SFP+ 10 Гбит/с	4x SFP+ 10 Гбит/с	2x SFP+ 10 Гбит/с	2x SFP+ 10 Гбит/с	2x SFP+ 10 Гбит/с	2x SFP+ 10 Гбит/с

1. Программно-аппаратный комплекс Diamond VPN/FW представляет собой UTM-решение, сочетающее в себе функции межсетевого экрана, VPN-шлюза, системы обнаружения вторжений (IDS) [5]. Входит в реестр отечественного ПО (№1425) и обладает действующим сертификатом ФСТЭК России №2260, подтверждающим соответствие требованиям руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» — по 2 классу защищенности. Обладает действующим сертификатом ФСБ России №124-2702 на соответствие требованиям к шифровальным (криптографическим) средствам класса КС1, КС2 и КС3 (в зависимости от вариантов исполнения) обладает СКЗИ Dcrypt 1.0, реализующее функции шифрования и ЭП в составе ПАК. Обеспечивает шифрование передаваемых данных по ГОСТ 28147-89, ГОСТ 34.10-2012, ГОСТ 34.11-2012 [6].

2. Программно-аппаратный комплекс ViPNet Coordinator HW представляет собой сертифицированный криптошлюз и межсетевой экран, обеспечивает шифрование данных, передаваемых по различным каналам связи с помощью построения VPN (как на сетевом, так и на канальном уровнях модели OSI – L3, L2 VPN) по ГОСТ 28147-89 и позволяет организовать защищенный доступ как в ЦОД, так и в корпоративную инфраструктуру. Функционирует на базе адаптированной ОС Linux [7].

ViPNet Coordinator HW обладает следующими особенностями: для построения VPN используется собственный протокол ViPNet VPN; поддержка централизованного управления и удаленного обновления с помощью ПО ViPNet Administrator; поддержка взаимодействия с клиентскими компонентами (ПО ViPNet Client) на различных операционных системах (Windows, Linux, macOS, iOS, Android). Входит в реестр отечественного ПО (№2798), обладает действующими сертификатами соответствия, в том числе:

ФСБ России №СФ/124-2981, подтверждающим выполнение требований к шифровальным (криптографическим) средствам класса КС3;

ФСБ России №СФ/525-3007, подтверждающим выполнение требований к межсетевым экранам 4 класса защищенности;

ФСТЭК России № 3692, удостоверяющий, что ПАК является межсетевым экраном типа «А» и соответствует требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016) и «Профиль защиты межсетевого экрана типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ».

3. Программно-аппаратные комплексы ALTELL NEO могут использоваться для исполнения разных сценариев: фильтрации трафика, защиты демилитаризованных зон (DMZ), создания защищенного канала связи по сетям общего пользования (VPN), предоставления защищенного доступа к локальной сети для мобильных пользователей, защиты персональных данных (152-ФЗ и приказа ФСТЭК №17 и №21), предоставление защищенного доступа в Интернет, защиты банковских терминалов и т. д. Входит в реестр отечественного ПО №382 [8].

ALTELL NEO 310 предназначен для крупных территориально-распределенных организаций, имеющих около 1 000 сотрудников. Представляет собой криптошлюз и межсетевой экран, обеспечивает шифрование данных, передаваемых по различным каналам связи с помощью построения VPN. Все модели межсетевых экранов ALTELL NEO имеют сертификаты ССС и Госстандарта России, ФСТЭК, ФСБ:

ФСБ России СФ/СЗИ-0074 04.10.2018 Межсетевой экран ALTELL NEO v. 1.5, по 4-му классу защищенности;

ФСТЭК России Межсетевой экран ALTELL NEO v. 2.0 на соответствие профилям защиты ИТ.МЭ.А2.ПЗ и ИТ.МЭ.Б2.ПЗ;

ФСТЭК России 2634 10.05.2018 Межсетевой экран ALTELL NEO v. 1.5, по 3-му классу защищенности и по 3-му уровню контроля отсутствия недекларированных возможностей;

ФСТЭК России 2726 01.10.2018 Межсетевой экран ALTELL NEO v. 1.5, по 2-му классу защищенности и по 2-му уровню контроля отсутствия недекларированных возможностей.

Подобранные для сравнения программно-аппаратные комплексы обладают необходимыми сертификатами соответствия и могут быть использованы в ЦОД для защиты передаваемых данных по каналам связи. Основным критерием выбора оборудования является его производительность, поэтому стоимостной расчет будет производиться только для моделей: ALTELL NEO 310 и ViPNet Coordinator HW5000.

Поскольку в оборудовании необходимо наличие 4 оптических сетевых интерфейсов SFP+, то преимуществом ViPNet Coordinator HW5000 является наличие 4 оптических сетевых интерфейсов SFP+ 10 Гбит/с в то время, как у ALTELL NEO 310 их 2, поэтому необходимо рассмотреть стоимость приобретения дополнительного модуля расширения.

Рассмотрим стоимость данных программно-аппаратных комплексов (табл.2).

Таблица 2. Сравнительный анализ стоимости программно-аппаратных комплексов
Table 2. Comparative analysis of the cost of software and hardware complex

	ViPNet Coordinator HW5000	ALTELL NEO 310
Стоимость оборудования, руб.	2 034 100	1 097 900
Стоимость модуля с двумя оптическими интерфейсами SFP+ для ALTELL NEO 310, руб.	–	112 500
Стоимость передачи прав на использование программного обеспечения	25% от стоимости оборудования	30% от стоимости оборудования

Проведем расчет приобретения программно-аппаратных комплексов.

ViPNet Coordinator HW5000 = 2 034 100 + 508 525 = 2 542 625 руб.

ALTELL NEO 310 = 1 097 900 + 112 500 + 329 370 = 1 539 770 руб.

ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Таким образом, приобретение программно-аппаратного комплекса ALTELL NEO 310 для ЦОД более целесообразно и выгодно. Данное

оборудование отвечает всем необходимым требованиям, отличается надежностью и эффективностью, высокой производительностью. Несмотря на необходимость закупки дополнительного модуля, затраты на приобретение существенно меньше, чем на продукт конкурентов.

ЛИТЕРАТУРА

1. Приказ Министерства Здравоохранения РФ № 911н от 24.12.2018 г. СПС КонсультантПлюс.
2. Методические рекомендации по обеспечению функциональных возможностей медицинских информационных систем медицинских организаций (МИС МО). СПС КонсультантПлюс.
3. Виртуализация. https://ru.wikipedia.org/wiki/Виртуализация.
4. Государственный контракт на оказание услуг виртуального центра обработки данных (ВЦОД) и защищенного канала связи для обеспечения функционирования Региональной медицинской информационной системы здравоохранения Ивановской области (РМИС СЗ ИО) и тиражирования ее функционала на учреждения здравоохранения Ивановской области в рамках реализации мероприятия: «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы здравоохранения (ЕГИСЗ)» № 01332000017190028260001/526.
5. Единое решение для защиты от сетевых угроз. https://www.tssltd.ru/products/diamond-vpn#teaser.
6. DIAMOND VPN/FW. Сертификаты. https:// www.tssltd.ru/products/diamond-vpn/certificates.
7. ViPNet Coordinator HW 4. Программно-аппаратный шлюз безопасности. https://infotecs.ru/product/version/vipnet-coordinator-hw/pokolenie-4/4-3-2.html#docs.
8. Аппаратный межсетевой экран ALTELL NEO — защита корпоративной, локальной сети. https://www.altell.ru/products/neo/.
9. «Профиль защиты межсетевых экранов типа А четвертого класса защиты ИТ.МЭ.А4.ПЗ». СПС КонсультантПлюс.
10. «Профиль защиты межсетевых экранов типа Б четвертого класса защиты ИТ.МЭ.Б4.ПЗ». СПС КонсультантПлюс.
11. «Профиль защиты межсетевых экранов типа В четвертого класса защиты ИТ.МЭ.В4.ПЗ». СПС КонсультантПлюс.
12. «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты ИТ.СОВ.С4.ПЗ». СПС КонсультантПлюс.
13. Цены на устройства ALTELL NEO (Firewall, VPN, UTM). https://www.altell.ru/products/neo/prices/.
14. Прайс-лист: программное обеспечение ViPNet, программно-аппаратные комплексы ViPNet, сертификаты активации сервиса технической поддержки ViPNet. https://infotecs.ru/product/prices.php.
15. Обзор вариантов реализации отказоустойчивых кластеров: Stratus, VMware, VMmanager Cloud. https://habr.com/ru/company/ispsystem/blog/313066/.
16. 7 мер защиты сервера. https://habr.com/ru/company/galtsystems/blog/314344/.
17. ЦОД повышенной ответственности. https://habr.com/ru/company/croc/blog/147474/.
18. Как устроен центр обработки данных. https://itglobal.com/ru-ru/company/blog/data-center-brief-explanation/.
19. Виртуализация и виртуальные дата-центры: Базовые вопросы. https://habr.com/ru/company/it-grad/blog/276807/.
20. Инфраструктура ЦОД на пальцах: оборудование, виртуализация, управление. https://storedigital.ru/2020/11/19/ infrastruktura-cod-na-palcax-oborudovanie-struktura-upravlenie/.

REFERENCES

1. Order of the Ministry of Health of the Russian Federation N 911n of 24.12.2018. CALR ConsultantPlus. (in Russian).
2. Methodological recommendations for ensuring the functionality of medical information systems of medical organizations. CALR ConsultantPlus. (in Russian).
3. Virtualization. https://ru.wikipedia.org/wiki/Virtualization. (in Russian).
4. State Contract N 01332000017190028260001/526 for the provision of services of a virtual data processing center and a secure communication channel to ensure the functioning of the Regional Medical Information System of the health System of the Ivanovo Region and the replication of its functionality to health institutions of the Ivanovo region as part of the implementation of the event: "Creation of a single digital circuit in healthcare on the basis of the unified state health information system». (in Russian).
5. A single solution to protect against network threats. https:// www.tssltd.ru/products/diamond-vpn#teaser (in Russian).
6. DIAMOND VPN/FW. Сертификаты. https://www.tssltd.ru/products/diamond-vpn/certificates. (in Russian).
7. ViPNet Coordinator HW 4. Программно-аппаратный шлюз безопасности. https://infotecs.ru/product/version/vipnet-coordinator-hw/pokolenie-4/4-3-2.html#docs. (in Russian).
8. Hardware firewall ALTELL NEO – protection of the corporate, local network. https://www.altell.ru/products/neo/ (in Russian).
9. «The protection profile firewall type A the fourth grade security IT.FW.A4.PP». CALR ConsultantPlus. (in Russian).
10. «The protection profile firewall type B the fourth grade security IT.FWB4.PP». CALR ConsultantPlus. (in Russian).
11. «The protection profile firewall type V the fourth grade security IT.FW.Q4.PP». CALR ConsultantPlus. (in Russian).
12. «The security profile of intrusion detection systems network-level fourth grade security IT.IDS.C4.PP». CALR ConsultantPlus. (in Russian).
13. Prices for ALTELL NEO devices (Firewall, VPN, UTM). https://www.altell.ru/products/neo/prices/ (in Russian).
14. Price list: ViPNet software, ViPNet hardware and software systems, ViPNet technical support service activation certificates. https://infotecs.ru/product/prices.php (in Russian).
15. Overview of implementation options for failover clusters: Stratus, VMware, VMmanager Cloud. https://habr.com/ru/company/ispsystem/blog/313066/ (in Russian).
16. 7 server security measures. https://habr.com/ru/company/galtsystems/blog/314344/ (in Russian).
17. Data center of increased responsibility. https://habr.com/ru/company/croc/blog/147474/ (in Russian).
18. How the data processing center works. https://itglobal. com/ru-ru/company/blog/data-center-brief-explantion/ (in Russian).
19. Virtualization and virtual data centers: Basic questions. https://habr.com/ru/company/it-grad/blog/276807/ (in Russian).
20. Data center infrastructure on your fingers: hardware, virtualization, management. https://storedigital.ru/2020/11/19/infrastruktura-cod-na-palcax-oborudovanie-struktura-upravlenie/ (in Russian).

Поступила в редакцию 13.07.2021
Принята к опубликованию 28.07.2021

Received 13.07.2021
Accepted 28.07.2021