УДК 004.056 Вестник УрФО № 3(49) / 2023, с. 54–60

Маслова М.А., Аветисян В.А.

DOI: 10.14529/secur230305

РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ УДАЛЕННОГО ПОДКЛЮЧЕНИЯ И ОБЛАЧНОГО ПРИСУТСТВИЯ[1]

Все более популярнее становятся облачные услуги как для пользователя, так и различного рода компаний. Поэтому поставщики облачных услуг стараются сделать как можно удобнее, защищённее свои услуги, вкладывая в это множество средств как финансовых, так и человеко-ресурсов. Инвестиции в данную отрасль дают возможность последующей волне миграции корпоративных приложений и формированию основы для нового программного обеспечения, уже основанного на искусственном интеллекте и новым возможностям роста рынка. Но помимо новых возможностей, идет большой рост рисков, связанных с данной областью. Поэтому в данной статье будут рассмотрены облачные сервисы, статистика развития, возможные риски и пути предупреждения и устранения.

Ключевые слова: *информационная безопасность, риски, облачные сервисы, облачные услуги.*

Maslova M.A., Avetisyan V.A.

INFORMATION SECURITY RISKS IN CONDITIONS OF REMOTE CONNECTION AND CLOUD PRESENCE

Cloud services are becoming more and more popular both for the user and various companies. Therefore, cloud service providers are trying to make their services as convenient and secure as possible, investing in this a lot of money, both financial and human resources. Investment in this industry is enabling the next wave of enterprise application migration and laying the groundwork for new software already based on artificial intelligence and new market growth opportunities. But in addition to new opportunities, there is a big increase in the risks associated with this area. Therefore, this article will consider cloud services, development statistics, possible risks and ways to prevent and eliminate them.

Keywords: *information security, risks, cloud services, cloud services.*

[1] Работа выполнена в рамках Соглашения от 30.06.2022 г. № 40469-21/2022-к.

Облачные сервисы становятся все популярнее и активнее, а скорость перехода для работы в них все больше, а безопасность стоит на втором месте. Хотя она должна быть основным параметром, так как злоумышленники в первую очередь ищут уязвимость именно здесь. Каждый день мы видим множество инцидентов, которые именно произошли в облачных средах по кражам данных как обычных пользователей, так и крупных компаний по различным причинам.

Рассмотрим основные риски информационной безопасности при использовании облака, возможные их средства защиты и возможные действия сведения их к минимуму.

В статье [1], были рассмотрены виды облаков и их описание. Какие же риски существуют для них и как они отличаются?

Рис. 1. Риски облачных сервисов

Рассмотрим подробнее каждый вид:

1) Частные облака

Одними из основных рисков данного направления относится построение качественной, безопасной системы, которая дает возможность обслуживать множество внутренних пользователей, а также поддерживать критичные ИС.

Если рассмотреть структуру упрощенного облака, то она включает в себя: набор инфраструктурных компонентов, платформу автоматизации частного облака, портал управления облачной инфраструктуры и непосредственно ресурсы, которые развернуты в самом облаке (рис. 2).

Если рассматривать инфраструктурные

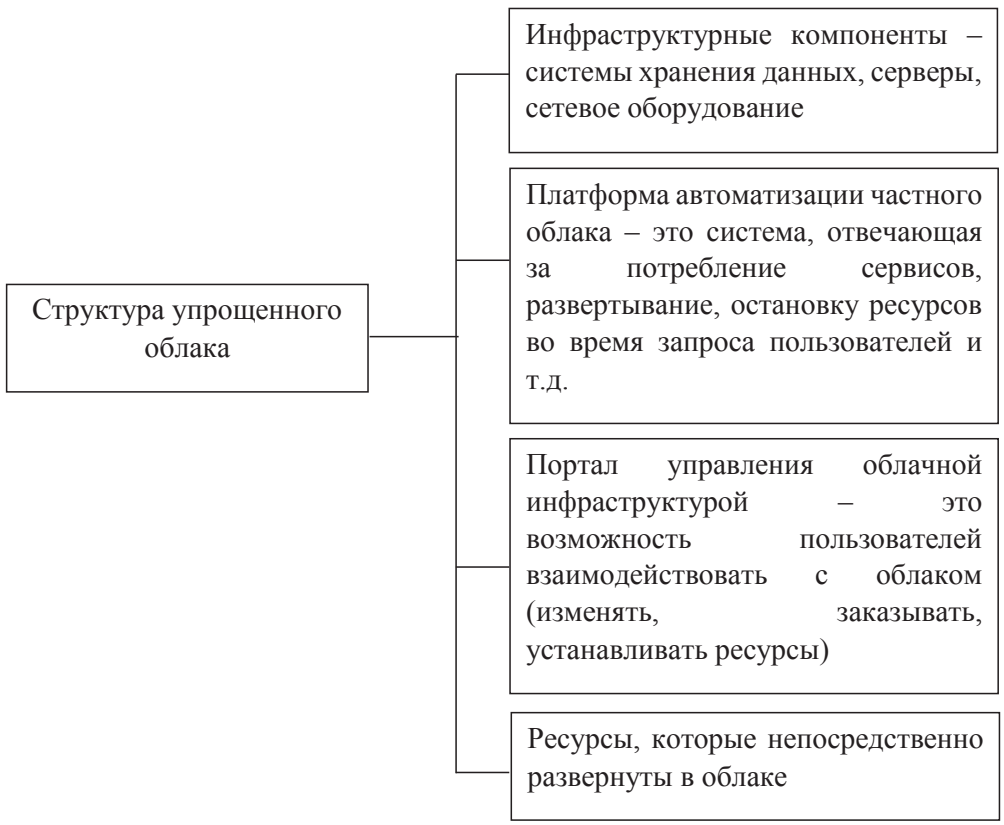

Рис. 2. Структура облака

компоненты, то особых свойств нет для того, чтоб обезопасить доступ к физ. инфраструктуре и выполнить резервирование ключевых компонентов. Но если же уже идет переход на уровень платформы автоматизации частного облака, тогда всплывают различные нюансы и риски, на которые необходимо заострить внимание, а именно:

– общая инфраструктура – необходимо ее разделить между пользователями так, чтоб они не имели доступа к другим ресурсам пользователей за счет реализации качественной модели управления доступом и разграничением ролей;

– перехват контроля над платформой автоматизации частного облака злоумышленником. Для невозможности реализации данного риска путем завладения всеми ресурсами, которые развернуты в облаке необходимо установить защиту сервисных учетных записей, которые используются платформой, проводить активный мониторинг сервисного пользования учетными записями, используемыми платформой, изменениями в данной конфигурации, а также проводить процесс усиления защищенности системы с целью снижения рисков от возможных угроз платформы используя все рекомендации вендора;

– использование уязвимых образов для развертывания ресурсов в облаке, которые злоумышленник может подменить – необходимо обеспечить всем виртуальным машинам, которые развернуты в работе облака качественный процесс развертывания инфраструктуры с постоянной проверкой качества и целостности используемых образов и установить защиту доступа к репозиторию доверенных образов;

– отказоустойчивость облачной платформы – данный риск влияет на все используемые информационные системы, которые развернуты в данном облаке. Для устранения необходимо проводить постоянное резервирование ключевых компонентов платформы и копирования данных;

– портал управления облачной инфраструктурой – несет риски по отношению к небезопасному управлению пользователями своими облачными средами. Для уменьшения данного риска необходимо как можно чаще проводить обучение сотрудников по правильной работе с облаком, выполнением обязательных рекомендаций и прописанных инструкций со сдачей дополнительного экзамена или теста; установить им роли и дать определенные доступы до необходимых им ресурсам, соответствующим их компетенциям;

– уровень ресурсов, развернутый в облаке, несет риски связанные со спецификой облака – при создании пользователями ресурсов в облаке есть риск неправильных настроек параметров безопасности, возможной ошибки при работе, риск постоянно меняющейся, создающейся и уничтожающейся информации, а также банальной невнимательности, приводящей к забывчивости в зашифровке данных, приводящих к плохой защите при доступе к ресурсам интернет. Тут необходимо внимательно следить за контролем действий, шифрования, изоляции компонентов ИС, реализации параметров безопасности на уровне ОС, разработки и внедрения шаблонов безопасных конфигураций, установки автоматических параметров безопасности.

Защита частного облака. Построение частного облака необходимо разделить на несколько частей: проектирование, развертывание и эксплуатация, которые содержат следующие задачи (таблица 1).

Все вышеперечисленные меры необходимы для организации работы частного облака и несут немалые вложения, но на безопасности экономить нельзя, так как повсеместная автоматизация использования облака дает много плюсов в работе: уменьшения рутинной работы персонала, развитие в упрощении работы особенно в контроле за безопасностью ИС организации или компании [2, 3].

2) Публичные облачные инфраструктуры

Структура публичного облака имеет схожую структуру с частным облаком, представленным на рис.2, отличие состоит лишь в том, что тут за инфраструктурные компоненты и платформу автоматизации отвечает не пользователь, а провайдер. Т.е. в данном случает риски информационной безопасности будут распределены. Провайдер будет отвечать за защиту и доступность облачной платформы и инфраструктуры самого облака, а пользователь за его использование в организации и безопасность развернутым систем в облаке. Т.е. тут самой организации в первую очередь необходимо обратить внимание на выбор провайдера, проанализировать его рейтинг в сфере защиты и обеспечения основных требований регуляторов.

Таблица 1

Задачи при построении частного облака

Этапы построения	Задачи
Проектирование	Необходимо определить: все уязвимости и важные компоненты в архитектуре облака; ролевую модель; необходимые элементы для закрытия встроенных компонентов облака и средств защиты; проводить оценку и контролировать период действий для имеющихся лицензий и оборудования заказчика.
Развертывание	Проверить существующие контроли безопасности, не было ли каких-либо важных отклонений от изначальной архитектуры, а также что бы были закрыты все учетные записи и доступы после выполненных работ.
Эксплуатация	Необходимо разработать: процедуры для поддержания безопасности облака во время работы с ним; требования к постоянной поддержке и необходимого обслуживания облака; инструкции к пользованию облаком внутри компании на разных уровнях пользования им и обеспечения постоянной безопасности облака; четкие организационные и технические меры и механизмы постоянного контроля безопасности при работе пользователей в облаке.

Риски также аналогичны с частным облаком, но еще и имеются дополнительные:

– избыточное использование ресурсов;

– возможность подключения разных пользователей и эту «дыру» необходимо тщательно закрыть. Необходимо установить ограничения на любые возможные подключения к облаку для всех устройств и сетей с обязательной аутентификацией пользователей, как минимум двухфакторной. Исключения остаются лишь для доверенных устройств и сетей [4, 5].

3) Облачные приложения

Данный вид характерен тем, что провайдер отвечает за все действия при работе с приложением, а пользователь отвечает лишь только за его использование в организации и настройки безопасности. Рекомендации по выбору провайдера такие же, как и в публичной облачной инфраструктуре. Риски, которые могут быть:

– обеспечение небезопасного доступа к облачному приложению, т.к. облачные сервисы дают возможность подключиться любому пользователю, поддерживает как гостевые, так и анонимные приложения, то это создает большие риски в безопасности. Тут так же необходимо ограничить доступ для всех анонимных подключений и оставить только безопасные подключения с помощью CASB или облачного приложения;

– пользователь выбирает и обеспечивает настройки безопасности используя в основном журналы сетевого оборудования, решения Cloud Access Security Broker, так как они содержат большую базу облачных приложений, которые автоматически обнаруживают их применение, могут выявлять пользователей организации, которые их используют и выдают передаваемые ими данные.

Так как в организациях используют не одно, а часто очень много облачных сервисов одновременно, тогда дополнительно необходимо разработать правила общего подхода к работе с облачными приложениями, который должен также выполнять все требования безопасности для всех этапов: выбора облачных приложений организации, внедрения, эксплуатация и вывода из использования. При выборе облачного приложения пользуются тем, что необходимо для работы в организации, а именно, что будет использоваться и для чего. Но важно помнить о интеграции его с единой системой управления учетными записями в организации, для контроля всех существующих и своевременного блокирования уже не работающих пользователей организации. Также важно реализовать все контроли безопасности и интегрировать приложения с системами безопасности организации для ее обеспечения безопасности и эксплуатации облачного сервиса; следить за актуальностью административных привилегий; постоянном мониторинге событий в облаке; обеспечить сохранность всех данных из облака и их дублирование [6, 7].

Приведем существующую статистику в данной области. Что касается мирового рынка инструментов защиты для облачных сред в 2022 году, то она также набрала обороты на 38% (т.е. возросла на 1 млрд. дол.) по результатам исследований от 15 марта 2023 г. компанией Dell'Oro Group [8].

Объем рынка SASE в 2022 г. по обнародованным данным Dell'Oro Group превысил 6 млрд. долларов, с увеличением роста в 34%

по отношению к предыдущему году. При этом рост данного рынка уже третий год составляет больше 30 %. Т.е. пандемия COVID-19 дала старт новым сервиса и рынкам, увеличила не только доходы компаний, но и дала толчок для модернизации сетей, архитектуры безопасности с постоянно увеличивающейся динамикой продаж, улучшенных услуг и инноваций.

В 2022 г рынок публичных облачных услуг значительно вырос по сравнению с 2021 г. по данным исследований IDC от 6 июля 2023 г. (см. рис. 3) и составил 22,9 %. В свою очередь выручка от основных облачных услуг, поддерживающих стратегий, которые ориентированы на цифровую трансформацию предприятия выросла до 28,8 %, что по мнению IDC очень повышает увеличивающую зависимость компаний от облачной инфраструктуры, инструментов искусственного интеллекта и сервисов высокопроизводительных вычислений.

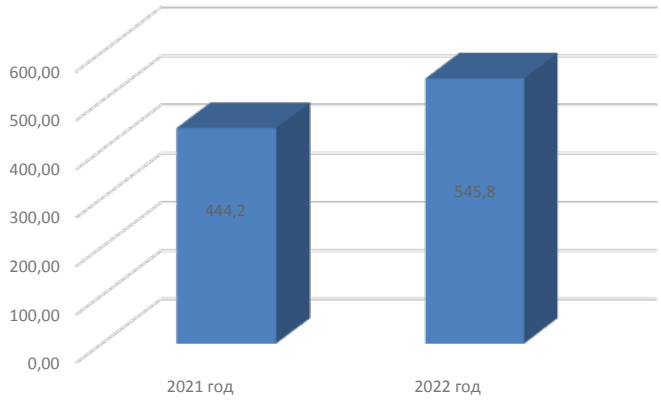

Рис. 3. Объем глобального рынка публичных облачных услуг, в млрд. дол.

Если смотреть по росту сегментов в 2022 г., то лидером стал сегмент инфраструктуры как услуги – IaaS и платформы как услуги PaaS и доход их составил суммарно 195 млрд долларов, что на 29% больше по отношению к 2021 г. Что же касается программного обеспечения как услуги SaaS и географически распределенной сетевой инфраструктуры CDN, то их затраты увеличились на 229 млрд. долларов, что составило 19% роста.

Если смотреть на динамику рынка облачных систем, то для их поддержания и развития операторы общедоступных облачных сервисов вложили 120 млрд долларов на оснащение, строительство, аренду инфраструктуры для развития своих центров обработки данных, что также больше, чем в 2021 году на 13%. Самыми крупными компаниями в общедоступной облачной экосистеме стали такие как Microsoft, Amazon, Salesforce, Google и др. и составило 60% всех доходов на эти компании, связанные с публичными облаками.

Если промониторить прогнозы динамики рынка для облачных систем, то они многообещающие, например, по данным Gartner за 2022 г мировые расходы конечных пользователей на общедоступные облачные сервисы выросли по сравнению с предыдущим годом на 77,7 млрд. долларов и составило 490, 33 млрд. долларов, где доля выручки распределилась по разным сервисам (рис. 4) [9, 10].

Чтоб быть в лидерах, компаниям необходимо быть гибкими и учитывать все изменения и тренды, например:

– развивать сервисы машинного обучения, искусственного интеллекта, работы с Big Data и базами данных,

– переводить как можно больше клиентов AWS на собственные процессоры,

– разрабатывать и адаптировать базы данных под определенные процессы,

– внедрять использование периферийных, облачных и 5G-сетей,

– охватывать большой спектр корпоративных IT-задач от SaaS до PaaS и IaaS,

– использовать облачные сервисы как часть стратегии цифровой трансформации,

– применять лучшие практики сервис-провайдеров публичных облаков в развитии своей IT-инфраструктуры, на основе частного облака или на базе пограничных вычислений,

– иметь постоянно растущий авторитет и инновации.

Рост данной области услуг будет продолжаться и доходы расти и по прогнозам Synergy Research Group к 2026 г они удвоятся, а крупные поставщики облачных услуг увеличат число действующих гипермасштабируе-

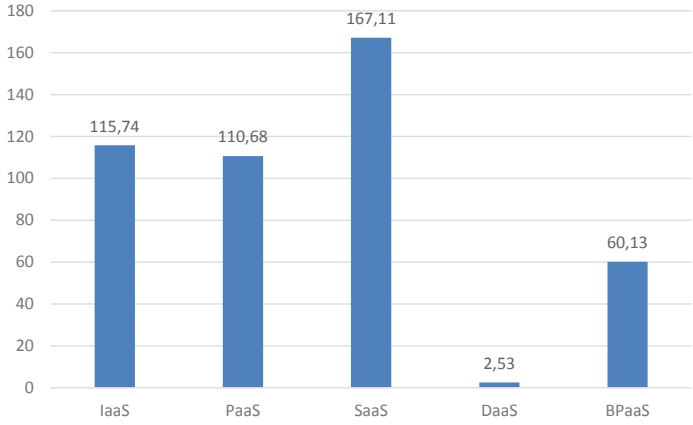

Рис. 4. Мировая доля выручки сервисов, млрд. долларов

мых центров обработки данных на 50%, с поднятием пропускной способности сетей более 65% [8].

Вывод. Благодаря пандемии открылись новые возможности в разных сферах жизнедеятельности человека, увеличилось количество рабочих мест удаленной работы, что повлекло к развитию и обеспечению все лучшей безопасности в облаке. Следовательно, возрос спрос на SASE – продукты, которые помогают обеспечивать эффективную защиту сети на разных уровнях, а также внутри и снаружи периметра сети. В основном на данный момент времени, ведущие компании – это американские, китайские, на их долю пришлось 8% всех доходов от облачных услуг и 16% мощностей гипермасштабируемых дата – центров.

Использование частных облаков для бизнеса, является не просто IT-задачей, а должно стать бизнес приоритетом и основой для дальнейшего развития и растущих потребностей бизнеса. Это позволит ускорить внедрение новых возможностей, продуктов, функционала, при этом снизить цену ошибок и затраченное время на тестирование бизнес идей с повышением точности прогнозов. Так же работа с клиентами и партнерами становиться проще и менее затратной как денежно, так и по времени, упрощается работа персонала.

Литература

1. Нестеренко, В. Р. Современные вызовы и угрозы информационной безопасности публичных облачных решений и способы работы с ними / В. Р. Нестеренко, М. А. Маслова // Научный результат. Информационные технологии. – 2021. – Т. 6, № 1. – С. 48-54.

2. Зубарев, И. В. Основные угрозы безопасности информации в виртуальных средах и облачных платформах / И. В. Зубарев, П. К. Радин // Вопросы кибербезопасности. – 2014. – № 2(3). – С. 40-45.

3. Полонский, А. М. Обеспечение безопасного удаленного доступа для сотрудников экономической сферы научно-промышленного предприятия / А. М. Полонский // Актуальные проблемы экономики и управления. – 2022. – № 1(33). – С. 30-41.

4. Герасимов, В. М. Необходимость комплексной системы защиты биометрического голосового отпечатка от воздействия кибермошенников в сети интернет / В. М. Герасимов, М. А. Маслова // Вестник Луганского государственного университета имени Владимира Даля. – 2022. – № 5(59). – С. 95-102.

5. Сыроватская, А. Е. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему / А. Е. Сыроватская, Т. Г. Абрамова // Современные проблемы лингвистики и методики преподавания русского языка в ВУЗе и школе. – 2022. – № 34. – С. 804-809.

6. Маслова, М. А. Проблемы облачных сервисов и методы защиты от рисков и угроз / М. А. Маслова, Е. С. Кузьминых // Научный результат. Информационные технологии. – 2022. – Т. 7, № 3. – С. 14-22.

7. Станислав Федотин Облачная НЕбезопасность и как с ней бороться URL: https://www.jetinfo.ru/oblachnaya-nebezopasnost-i-kak-s-nej-borotsya/

8. Облачные вычисления (мировой рынок) URL: https://www.tadviser.ru/index.php/

9. https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023

10. https://www.srgresearch.com/articles/total-public-cloud-revenues-jumped-21-in-2022-surpassing-500-billion-despite-economic-headwinds

References

1. Nesterenko, V. R. Sovremennyye vyzovy i ugrozy informatsionnoy bezopasnosti publichnykh oblachnykh resheniy i sposoby raboty s nimi / V. R. Nesterenko, M. A. Maslova // Nauchnyy rezul'tat. Informatsionnyye tekhnologii. – 2021. – T. 6, № 1. – S. 48-54.

2. Zubarev, I. V. Osnovnyye ugrozy bezopasnosti informatsii v virtual'nykh sredakh i oblachnykh platformakh / I. V. Zubarev, P. K. Radin // Voprosy kiberbezopasnosti. – 2014. – № 2(3). – S. 40-45.

3. Polonskiy, A. M. Obespecheniye bezopasnogo udalennogo dostupa dlya sotrudnikov ekonomicheskoy sfery nauchno-promyshlennogo predpriyatiya / A. M. Polonskiy // Aktual'nyye problemy ekonomiki i upravleniya. – 2022. – № 1(33). – S. 30-41.

4. Gerasimov, V. M. Neobkhodimost' kompleksnoy sistemy zashchity biometricheskogo golosovogo otpechatka ot vozdeystviya kibermoshennikov v seti internet / V. M. Gerasimov, M. A. Maslova // Vestnik Luganskogo gosudarstvennogo universiteta imeni Vladimira Dalya. – 2022. – № 5(59). – S. 95-102.

5. Syrovatskaya, A. Ye. Kompleksnoye obespecheniye informatsionnoy bezopasnosti pri realizatsii ugrozy popytki dostupa v udalennuyu sistemu / A. Ye. Syrovatskaya, T. G. Abramova // Sovremennyye problemy lingvistiki i metodiki prepodavaniya russkogo yazyka v VUZe i shkole. – 2022. – № 34. – S. 804-809.

6. Maslova, M. A. Problemy oblachnykh servisov i metody zashchity ot riskov i ugroz / M. A. Maslova, Ye. S. Kuz'minykh // Nauchnyy rezul'tat. Informatsionnyye tekhnologii. – 2022. – T. 7, № 3. – S. 14-22.

7. Stanislav Fedotin Oblachnaya NEbezopasnost' i kak s ney borot'sya URL: https://www.jetinfo.ru/oblachnaya-nebezopasnost-i-kak-s-nej-borotsya/

8. Oblachnyye vychisleniya (mirovoy rynok) URL: https://www.tadviser.ru/index.php/

9. https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600- billion-in-2023

10. https://www.srgresearch.com/articles/total-public-cloud-revenues-jumped-21-in-2022-surpassing-500-billion-despite-economic-headwinds

---

МАСЛОВА Мария Александровна, старший преподаватель кафедры «Информационная безопасность», Севастопольский государственный университет. Россия, 299053, г. Севастополь, Университетская улица, дом 33.; младший научный сотрудник, Федеральное государственное автономное образовательное учреждение высшего образования Ростовский государственный экономический университет (РИНХ). Россия, 344002, г. Ростов-на-Дону, ул. Большая Садовая, д. 69. E–mail: mashechka–81@mail.ru

MASLOVA Maria Aleksandrovna, Senior Lecturer, Department of Information Security, Sevastopol State University. Russia, 299053, Sevastopol, Universitetskaya street, 33.; junior researcher Federal State Autonomous Educational Institution of Higher Education Rostov State University of Economics (RINH). Russia, 344002, Rostov-on-Don, st. Bolshaya Sadovaya, 69. E-mail: mashechka–81@mail.ru

АВЕТИСЯН Владимир Арменович, аспирант кафедры «Информационная безопасность» Автономная некоммерческая организация высшего образования «Белгородский университет кооперации, экономки и права». Россия, 308023, г. Белгород, ул. Садовая дом 116-а. E-mail: avetisyan.vladimir25@yandex.ru.

AVETISYAN Vladimir Armenovich, postgraduate student of the Information Security Department Autonomous Non-Commercial Organization of Higher Education Belgorod University of Cooperation, Economics and Law. Russia, 308023, Belgorod, Sadovaya Street, 116-a. E-mail: avetisyan.vladimir25@yandex.ru.