УДК 338.28+004.056.5

ЗАБЕЗПЕЧЕННЯ ПОЛІТИКИ БЕЗПЕКИ ХМАРНИХ ERP-СИСТЕМ

Нємкова Олена Анатоліївна,
кандидат фізико-математичних наук, доцент,
доцент кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка»
e-mail: cyberlbi12@gmail.com

Наумов Олег Вадимович,
аспірант
ДВНЗ «Університет банківської справи»
e-mail: keeperoleg26@gmail.com

Анотація. Проаналізовано можливості забезпечення політики безпеки підприємства сучасними хмарними ERP-системами. Розглянуто стан засобів інформаційної безпеки, що надають хмарні ERP-системи зі списку топ-10. Показано, що забезпечення інформаційної безпеки хмарними ERP-системами стосується захисту інформаційних ресурсів підприємства від зовнішніх загроз, а саме — менеджменту прав доступу, безпеці транспортного рівня і захисту від мережевих атак. За наявності доступу до журналів логів і файлів даних не розвинуто технологій виявлення інцидентів порушення політики безпеки і формування сигналу тривоги. Захист від витоку інформації з підприємства хмарними ERP-системами не забезпечується. Також розглянуто можливості перенесення у хмару систем, що запобігають витоку інформації з підприємства, так званих DLP-систем. Проаналізовано сервіси конкретних DLP-систем, що є на українському ринку. Досліджено, що повноцінних хмарних аналогів локальним DLP-системам немає. Для перенесення DLP-системи у хмару і створення «DLP як сервіс» локальна система має бути трансформована. Частина системи, що забезпечує перевірку дій на робочих комп'ютерах, має залишитися на локальному рівні. У хмару може бути перенесена частина системи, яка фіксує виток інформації через канали зв'язку (Інтернет, Skype та інші), а також база проіндексованої інформації, сервіс налаштування політики безпеки і центр формування сигналу тривоги. Усе це призведе до нових технічних вимог на канали зв'язку, необхідності використовувати послуги хмарного брокера з відповідними сертифікатами безпеки, а також суттєвого підвищення вартості експлуатації хмарних послуг. Проведене оцінювання вартості послуг наявних хмарних DLP-систем показало, що підприємство не може контролювати повністю весь потік інформації внаслідок дуже високої ціни. Таким чином, для ефективної роботи хмарних DLP-систем потрібна постійна активна участь співробітників інформаційної безпеки підприємства. Плюсами майбутніх хмарних DLP-систем є забезпечення підприємства потужностями для зберігання проіндексованих даних і розвиненими технологіями пошуку інцидентів політики безпеки.

Ключові слова: виток інформації, політика безпеки, інцидент інформаційної безпеки, хмарна ERP-система, DLP як сервіс, хмарний брокер.

Формул: 0; рис.: 0; табл.: 0; бібл.: 16.

PROVIDING CLOUD SECURITY POLICY FOR ERP-SYSTEMS

Nyemkova Elena,
Ph. D. in Physics and Mathematics, Associate Professor,
Associate Professor at the Department of Information Technology Security
of the National University «Lviv Polytechnic»
e-mail: cyberlbi12@gmail.com

Naumov Oleg,
Ph. D. student
of the SHEI «Banking University»
e-mail: keeperoleg26@gmail.com

Abstract. The article is devoted to the analysis of the possibilities of ensuring the security policy of an enterprise with modern cloud-based ERP-systems. The information security technologies that are available in the cloud ERP-systems from the list of top10 are considered. It is shown that these technologies are aimed at protecting the information resources of the enterprise from external threats and include the management of access rights, ensuring the security of the transport level and protection against network attacks. Technologies for detecting incidents of security policy and alarm generation are not used, although there is a possibility to access logs and data files in cloud ERP-systems. Information leakage protection from the enterprise by cloud ERP-systems is not provided. Also, the possibility of

transferring to the cloud of systems that prevent information leaks from the enterprise, the so-called DLP-systems are considered. The services of specific DLP-systems presented on the Ukrainian market have been analyzed. It is proved that there are no full-fledged cloud analogs to local DLP-systems. The local system must be transformed to transfer the DLP-system to the cloud and create "DLP as a service". The part of the system that provides verification of actions on work computers must remain at the local level. The part of the system that records information leaks through communication channels (Internet, Skype and others), as well as the database of indexed data, the security policy setting service and the alarm generation center can be transferred to the cloud. All this will lead to new technical requirements for communication channels, the need to use the services of a cloud broker with appropriate security certificates, as well as a significant increase in the cost of operating cloud services. The assessment of the cost of services of existing cloud DLP-systems showed that the company cannot fully control the entire flow of information due to the very high price. In addition, continuous updating of the security policy verification rules is necessary, which can only be carried out by an enterprise security officer. Thus, the continued active participation of information security officers is necessary for the effective operation of cloud DLP-systems. Providing the enterprise by the capacity to store indexed data and advanced technologies to search for incidents of security policy are advantages of future cloud DLP-systems.
Keywords: information leak, security policy, information security incident, cloud-based ERP-system, DLP as a service, cloud broker.

Formulas: 0; fig.: 0; tabl.: 0; bibl.: 16.

ОБЕСПЕЧЕНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ERP-СИСТЕМ

Немкова Елена Анатольевна,
кандидат физико-математических наук, доцент,
доцент кафедры безопасности информационных технологий
Национального университета «Львовская политехника»
e-mail: cyberlbi12@gmail.com

Наумов Олег Вадимович,
аспирант,
ГВУЗ «Университет банковского дела»
e-mail: keeperoleg26@gmail.com

Аннотация. Посвящено анализу возможностей обеспечения политики безопасности предприятия современными облачными ERP-системами. Рассмотрены технологии обеспечения информационной безопасности, которые имеются в наличии в облачных ERP-систем из списка топ-10. Показано, что эти технологии направлены на защиту информационных ресурсов предприятия от внешних угроз и включают менеджмент прав доступа, обеспечение безопасности транспортного уровня и защиту от сетевых атак. При возможностях доступа к журналам логов и файлов данных в облачных ERP-системах не используются технологии обнаружения инцидентов политики безопасности и формирования сигнала тревоги. Защита от утечки информации с предприятия облачными ERP-системами не обеспечивается. Также рассмотрены возможности переноса в облако систем, предотвращающих утечки информации с предприятия, так называемых DLP-систем. Проанализированы сервисы конкретных DLP-систем, представленных на украинском рынке. Доказано, что полноценных облачных аналогов локальным DLP-системам нет. Для переноса DLP-системы в облако и создания «DLP как сервис» локальная система должна быть трансформирована. Часть системы, которая обеспечивает проверку действий на рабочих компьютерах, должена остаться на локальном уровне. В облако может быть перенесена та часть системы, которая фиксирует утечку информации через каналы связи (Интернет, Skype и другие), а также база проиндексированных данных, сервис настройки политики безопасности и центр формирования сигнала тревоги. Все это приведет к новым техническим требованиям на каналы связи, необходимости использовать услуги облачного брокера с соответствующими сертификатами безопасности, а также существенному повышению стоимости эксплуатации облачных услуг. Проведенная оценка стоимости услуг существующих облачных DLP-систем показала, что предприятие не может контролировать полностью весь поток информации вследствие очень высокой цены. К тому же необходимо постоянное обновление правил проверки политики безопасности, что может выполнять только офицер безопасности предприятия. Таким образом, для эффективной работы облачных DLP-систем необходимо постоянное активное участие сотрудников информационной безопасности. Плюсами будущих облачных DLP-систем является обеспечение предприятия мощностями для хранения проиндексированных данных и развитыми технологиями поиска инцидентов политики безопасности.
Ключевые слова: утечка информации, политика безопасности, инцидент информационной безопасности, облачная ERP-система, DLP как сервис, облачный брокер.

Формул: 0; рис.: 0; табл.: 0; библ.: 16.

Вступ. Хмарну ERP-систему можна подати як модель для забезпечення зручного доступу по мережі до конфігурованих обчислювальних ресурсів (мереж, серверів, сховищ, додатків і служб), що відтворюють локальну ERP-систему. Технології хмарних ERP-систем можуть бути реалізовані в різноманітних архітектурних рішеннях, різних моделях обслуговування і розгортання: наприклад, модель обслуговування – програма як послуга (SaaS – Software-as-a-Service), модель розгортання — гібридна хмара (hybrid cloud), приватна хмара (private cloud) або хмара спільноти (community cloud). Спільною рисою є питання безпеки, що повинні відповідати як сучасним вимогам і стандартам, так і політиці безпеки конкретного підприємства — банку, промислового підприємства та інших.

Традиційні моделі безпеки на перший погляд не відповідають принципам хмарних обчислень, коли вся інформація про підприємство, його бізнес-процеси, маркетингові рішення перебуває поза його периметром. Але процеси глобалізації призвели до того, що окремі бізнес-процеси, їхні логістика та управління одного підприємства можуть бути розташовані на значній віддалі, тобто без використання інформаційних мереж їхнє функціонування було б неможливим. Досягнення у сфері безпеки протоколів передавання інформації, процедур автентифікації і авторизації для доступу до ресурсів, криптографічного захисту баз даних, постійного оновлення антивірусного захисту забезпечують надійне підґрунтя для безпечної віддаленої роботи офісів і виробничих потужностей. Фактично формат елементів безпеки інформаційних технологій для локальних мереж і серверів перенесено у хмарні технології.

Безпека хмарних сервісів в основному скерована на захист інформаційних ресурсів від зовнішніх загроз. Але кожне окреме підприємство повинно мати розроблену і затверджену політику безпеки, яка вимагає особливого підходу для хмарних реалізацій. Слід підкреслити дуже важливе значення політики безпеки для тих підприємств, де вагомим є людський фактор. Однозначно до таких підприємств відносять банківські установи, гіпермаркети, виробничі потужності з технологічними процесами, специфіка яких не підлягає розголошенню. Політика безпеки для сучасних підприємств є необхідним елементом, що має бути реалізованим у хмарних технологіях.

Аналіз досліджень і постановка завдання. Поява хмарних технологій призвела до розроблення низки стандартів з інформаційної безпеки у 2009—2011 роках, серед яких перш за все потрібно назвати стандарти NIST (National Institute of Standards and Technology) [1—3]. Основні положення, що сформульовано в цих документах, залишаються актуальними і на наш час. По-перше, безпека і конфіденційність є критерієм вибору постачальника хмарних послуг. По-друге, потрібна чітка фіксація договірних вимог, у тому числі положень про конфіденційність і безпеку. По-третє, потрібний постійний моніторинг стану безпеки хмарних послуг.

Національний центр кібербезпеки (NCCoE) у NIST побудував лабораторне середовище з використанням комерційних технологій і хмарних сервісів для формулювання рекомендацій із практики кібербезпеки [4].

Основні постачальники хмарних послуг, такі як SAP, Oracle, що займаються також розробленням інформаційної безпеки хмарних сервісів, надають результати досліджень у формі опису їхньої продукції [5; 6].

Велика кількість дослідників займається питаннями, пов'язаними з безпекою хмарних технологій, в основному їхні дослідження стосуються або конкретних питань, пов'язаних з інцидентами інформаційної безпеки хмарних сервісів, або присвячені системним питанням, наприклад, безпеці мережі і баз даних, безпеці на рівні сервера додатків, захисту інформації на клієнтському рівні [7—10].

Таким чином, дослідження в області хмарної безпеки в основному стосуються захисту інформаційних ресурсів підприємства від зовнішніх загроз, а питанням захисту від витоку інформації та захисту від інсайдерів не було приділено уваги.

Метою статті є аналіз можливостей забезпечення політики безпеки хмарних ERP-систем.

Результати дослідження. Компанії — постачальники хмарних рішень ERP-систем проводять дослідження питань інформаційної безпеки, щоб з'ясувати ситуацію на ринку. Дослідження компанії SAP (компанія вважається лідером серед топ-10 компаній — постачальників хмарних ERP-систем) показало, що 76 % організацій зазнали інцидентів у сфері безпеки. Разом з тим спостерігається перевантаження попереджень про інциденти: у середніх компаніях надходить майже 17 000 сповіщень про інциденти на тиждень, з них лише 19 % є надійними, розслідуваними — 4 %. До того ж брак кваліфікованого персоналу з кібербезпеки становить 66 %. Унаслідок цього тільки 14 % підприємств вважає, що традиційні засоби безпеки достатньо надійні для функціонування хмарних ERP-систем [11].

За дослідженням IBM на глобальному ринку в 77 % компаній немає аварійного плану реагування на кібератаку (cybersecurity incident response plan, CSIRP). У ході дослідження представники IBM опитали 2 800 фахівців з інформаційної безпеки з усього світу. За замовчуванням офіційно оформлений план CSIRP вважається основним інструментом захисту від кібератак, однак більшість респондентів відповіли, що в їхній компанії існують тільки неформальний набір правил або кожного разу IT-команда діє за ситуацією [12].

Надійність роботи хмарних ERP-систем забезпечується пакетами програм для управління, балансування й оптимізації ресурсів підприємства. Для забезпечення інформаційної безпеки в ERP-системах доступ до ресурсів користувачам надається на основі моделі RBAC (Role Based Access Control — керування доступом на основі ролей), широко використовуються криптографічні програмні засоби.

Проаналізуймо сервіси безпеки, що надаються провідними компаніями — постачальниками хмарних ERP-систем. Для аналізу обрано перші дві компанії зі списку топ-10 компаній — постачальників хмарних ERP-систем: компанію SAP і компанію Oracle [13].

Отже, безпека інформаційних ресурсів починається з прав доступу, тому SAP пропонує інфраструктуру управління корпоративною ідентифікацією — SAP ID Service, яка надається за замовчуванням для платформи SAP Cloud Platform. Дозволи доступу до додатків можуть бути згруповані для спрощення адміністрування. Якщо система ідентифікації вже існує (система IdP), SAP Cloud Platform представляє функції єдиного входу (SSO) і об'єднання ідентифікаторів. У хмарній платформі SAP ідентифікаційна інформація не зберігається на самій платформі SAP Cloud Platform, що підвищує рівень безпеки. Платформа допускає інший IdP для кожного субрахунку. У середовищі Cloud Foundry розробники додатків створюють і розгортають артефакти авторизації на основі додатків для бізнес-користувачів. Адміністратори можуть використовувати цю інформацію для призначення ролей, створення колекцій ролей і призначення цих колекцій бізнес-користувачам або групам користувачів.

Для підтримки безпеки транспортного рівня (TLS) SAP Cloud Platform використовує зашифровані канали зв'язку на основі протоколу HTTPS/TLS. Усі платформи, запущені до 1 липня 2018 року, підтримували всі три версії протоколу TLS: 1.0, 1.1 і 1.2. Після 1 липня 2018 року платформи підтримують тільки безпечнішу версію — TLS 1.2.

Для захисту від мережевих атак SAP Cloud Platform надає кілька механізмів захисту: захист від міжсайтових сценаріїв (Cross-Site Scripting), захист від атак на боці сервера (Server-Side Injection Attacks), захист від підробки міжсайтових запитів (Cross-Site Request Forgery) [14].

Таким чином, на нинішній день SAP Cloud Platform забезпечує менеджмент прав доступу, безпеку транспортного рівня і захист від мережевих атак.

Платформа моніторингу хмарних сервісів Oracle дозволяє ефективно знаходити причини різних проблем через аналіз лог-файлів і забезпечує можливість планування ресурсів IT-ландшафту: вимірювати завантаження баз даних і серверів додатків, оцінювати і прогнозувати реальне використання ресурсів центральних процесорів (CPU), пристроїв введення-виведення інформації (I/O), пам'яті.

Серед ключових можливостей інструментів Oracle Management Cloud щодо безпеки від витоку є: аналіз метрик і подій, агрегування даних журналів, автоматизоване виявлення аномалій і першопричин інцидентів. Вихідними даними для інструментів моніторингу є лог-файли, дані, що породжуються користувачами, машинні дані, файли трасувань, метрики продуктивності, діагностичні дані з репозиторію EM, журнали аудиту і т. д. Для аналізу поточного IT-ландшафту призначений сервис IT Analytics. Цілі цього сервісу — виявлення проблемних ділянок і порівняння навантажень у різні періоди, а також виявлення максимального споживання ресурсів за різними вимірами. Можливість візуалізації даних дозволяє спростити пошук за різними критеріями.

Отже, хмарне рішення від Oracle містить сервіси, що дозволяють доступитись до журналів логів і файлів даних, але для перевірки політики безпеки потрібно мати можливість у реальному часі виявляти і збирати дані, які мали б свідчити про порушення — інциденти. Також потрібно мати сервіс для формування сигналу тривоги. У цьому напрямі працюють компанії Tripwire, Belden і Claroty, які об'єднались для створення інформаційного продукту, що поєднує можливості управління журналом логів із неперервним виявленням загроз. Продукт призначений для виявлення інцидентів у промислових мережах (ICS-мережі), але застосовані підходи цілком можуть бути використані для систем запобігання витоків [15]. Для виявлення інцидентів застосований принцип машинного навчання на позитивних і негативних тестах. Для подальшої фільтрації застосовують кореляційні методи. Сервіс Tripwire Visibility містить також тестування для виявлення злому паролів і активності сканування, що використовують хакери для дослідження мережі, яку вони планують атакувати. Tripwire Visibility поставляється з великою колекцією попередньо сконфігурованих тестів для подій, які відбуваються в більшості мереж. Кореляційні тести також можуть бути легко написані споживачами.

Для проведення аналізу і контролю над конфіденційною інформацією використовують DLP-системи (Data Loss Prevention). На ринку України представлено кілька DLP-систем: Symantec DLP, McAfee Data Loss Prevention Endpoint 10.0, Контур інформаційної безпеки SearchInform та інші. Для прикладу розглянемо Контур інформаційної безпеки SearchInform, що призначений для ефективного захисту від витоків інформації [16]. Він використовується в різноманітних організаціях — від банків до великих промислових підприємств. Мета роботи Контура — виявлення інцидентів політики безпеки підприємства. Програмні агенти Контура SearchInform виконують тіньове копіювання всіх інформаційних пакетів і відстежують операції з файлами, а саме: відправлених на друк документів, переговорів у Skype; інформації, що записується на флеш-пам'ять, передавання даних за FTP-протоколом. Перехоплені повідомлення індексують і переносять у базу даних Microsft SQL Server. Далі за допомогою програми SearchInform AlertCenter проіндексовані дані перевіряють на відповідність заздалегідь налаштованим політикам безпеки. Розклад перевірок і перелік запитів налаштовують працівники служби безпеки організації. У разі виявлення збігів SearchInform AlertCenter негайно інформує про це службу безпеки підприємства.

Хмарного аналога Контур SearchInform на нинішній день немає. Якщо переносити DLP-систему в хмару, то для збереження функціоналу і глибини аналізу інформаційних пакетів вона має бути трансформована. Частина системи (агенти, що виявляють витоки через операції з файлами на локальних комп'ютерах і кінцевих точках) має залишитись на локальному рівні на робочих комп'ютерах. У хмару може бути перенесено агенти, що працюють з витоками через канали зв'язку, а також базу Microsft SQL Server проіндексованих даних, центр формування сигналу тривоги AlertCenter. Усе це призведе до нових технічних вимог на канали зв'язку, а також необхідності використовувати

послуги хмарного брокера з відповідними сертифікатами безпеки. Поява хмарного брокера обумовлена потребою одночасного використання підприємством двох різних хмар Saas — хмарної ERP-системи і хмарної DLP-системи.

У цілому, хмарні технології в Україні набувають популярності. Перш за все компанії, що планують перейти у хмари, цікавить функціонал системи і ціна впровадження. Наведемо деяки цифри. Вартість системи BAS (Busines Automatiom Software — рішення SAP для України) становить 180 000 грн. Вартість системи Clobbi (спільна розробка Великобританії і України з використанням 28-річного досвіду впровадження ERP-систем) складається з двох частин — це вартість обраних додатків функціоналу і вартість одночасного доступу потрібної кількості користувачів. Для 150 користувачів і доволі повного функціоналу вартість становить 6 705 доларів США (отримано за допомогою онлайн-калькулятора на сайті https://clobbi.com/ru/pricing/), що в перерахунку на гривні становить 187 740 грн за курсу 28 грн/дол., тобто системи BAS ERP і Clobbi мають однаковий порядок вартості для середнього бізнесу.

Вартість наявних хмарних DLP-систем, наприклад, Cloud Data Loss Prevention (DLP) API, залежить від обсягу перевірених даних і може ставати непомірною (набагато перевищувати вартість хмарної ERP-системи), якщо перевіряти всі потоки даних (як це відбувається для локальних DLP-систем). Тому постачальники рекомендують обмежити обсяг інформації, яку перевіряють. Зауважимо, що ціни на розглянуті локальні DLP-системи коливаються в дуже широкому діапазоні залежно від функціональних сервісів і кількості робочих комп'ютерів, на які встановлюються агенти.

Наступні дослідження будуть присвячені деталізації інформаційних потоків у хмарній DLP-системі і можливостям взаємодії хмарних систем ERP як послуга і DLP як послуга.

Висновки. Основні технічні та організаційні проблеми забезпечення захисту у хмарній ERP-системі від внутрішніх загроз багатьох підприємств полягає у складності структури їхніх корпоративних мереж. Наявні локальні рішення DLP-систем базуються на аналізі інформаційних потоків між серверами і кінцевими точками, а також активністю персоналу на робочих комп'ютерах. Для розвинутої системи захисту від витоку інформації всі потоки повинні перехоплюватись і зберігатись для подальшого аналізу. Зменшення обсягу інформації досягається завдяки її індексуванню, але все одно цей обсяг є дуже великим, він залежить від кількості робочих комп'ютерів. Для застосування вже наявних рішень систем запобігання витоку потрібно врахувати збільшення хмарних витрат на зберігання проіндексованої інформації, додаткові сервери для її обробки, збільшення смуги пропускання зовнішнього каналу зв'язку, а також необхідність єдиного входу у хмарну ERP-систему. Важливим моментом є затримка часу між моментом, коли інцидент відбувся, і моментом його виявлення.

Для рішення «DLP як сервіс» агенти збору подій, здебільшого, повинні бути розташовані на власній території підприємства, а у хмарі можуть бути розміщені архів інцидентів і засоби налаштування політики безпеки. Також провайдери хмарних DLP-систем і хмарні брокери мають бути відповідно сертифіковані.

Забезпечення політики безпеки вимагає постійного моніторингу інцидентів. Також потрібні великі зусилля на підтримку актуального стану політики безпеки. Якщо застосування хмарного рішення ERP-системи в основному знімає питання захисту від зовнішніх загроз, то внутрішні загрози і політика безпеки завжди залишаються проблемами самого підприємства. Це вимагає наявності висококваліфікованих спеціалістів із забезпечення політики безпеки і виявлення внутрішніх інцидентів.

Список використаної літератури

1. Badger L. DRAFT Cloud Computing Synopsis and Recommendations [Electronic resource] / L. Badger, T. Grance, R. Patt-Corner, J. Voas // NIST. — 2011. — May. — 86 p. — Available at : http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf.
2. Challenging Security Requirements for US Government Cloud Computing Adoption (Draft) [Electronic resource] // NIST. — 2011. — November. — 68 p. — Available at : http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Requirements_for_US_Government_Cloud.pdf.
3. Jansen W. Guidelines on Security and Privacy in Public Cloud Computing [Electronic resource] / W. Jansen, T. Grance // NIST. — 2011. — December. — 80 p. — Available at : https://csrc.nist.gov/publications/detail/sp/800-144/final.
4. Dodson D. Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments Relevance [Electronic resource] / D. Dodson, D. Carroll, G. Scinta, H. Prafullchandra, H. Singh, R. Yeluri et al. // NIST. — 2018. — August. — 4 p. — Available at : https://csrc.nist.gov/publications/detail/sp/1800-19/draft.
5. SAP Cloud Platform [Electronic resource]. — Available at : https://help.sap.com/viewer/65de2977205c403bbc107264b8eccf4b/Cloud/en-US/eb70f16b420447b6b33dedc3ebcf91cc.html.
6. Oracle. Cloud Security Ebook [Electronic resource]. — Available at : https://www.oracle.com/security/index.html.
7. Булдакова Т. И. Обеспечение информационной безопасности ERP-систем / Т. И. Булдакова, А. В. Коршунов // Вопросы кибербезопасности : спецвып. — 2015. — № 5 (13) — С. 41—44.
8. Catteddu D. Cloud Computing Benefits, risks and recommendations for information security [Electronic resource] / D. Catteddu, G. Hogben // The European Network and Information Security Agency. — 2009. — November. — 50 p. — Available at : https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security.

9. Patel A. An Intrusion Detection And Prevention System In Cloud Computing: A Systematic Review / A. Patel, M. Taghavi, K. Bakhtiyari, J. Celestino // Júnior Journal of Network and Computer Applications. — 2013. — Vol. 36. — Is. 1. — P. 25—41.
10. SAP Cloud Platform [Electronic resource]. — 2422 p. — Available at : https://help.sap.com/doc/bd6250c40c9c4c5391e3009a6f26dc3b/Cloud/en-US/SAP_Cloud_Platform.pdf.
11. SAAS Security: Best Practices for Minimizing Risk in the Cloud [Electronic resource]. — 11 p. — Available at : https://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/saas-security-best-practices-minimizing-risk-in-the-cloud-paper.html.
12. Сайт CNEWS. Экспертиза REDSYS. У 77 % компаний нет аварийного плана реагирования на кибератаки [Электронный ресурс]. — 2018. — Режим доступа : http://redsys.cnews.ru/news/top/2018-05-24_u_77_kompanij_net_avarijnogo _plana_reagirovaniya.
13. Panorama consulting solutions. 2019 Top 10 Distribution ERP Systems Report [Electronic resource]. — 14 p. — Available at : https://cdn2.hubspot.net/hubfs/4439340/Top-10-Distribution-ERP-Systems-2.pdf.
14. SAP Help Portal. Protection from Web Attacks [Electronic resource]. — Available at : https://help.sap.com/viewer/65de2977205c403bbc107264b8eccf4b/Cloud/en-US/52750a8f86bb428ca224daa4312d122e.html.
15. The State of Security. Tripwire Visibility for ICS: Getting From Data Mountains to Event Nuggets [Electronic resource]. — Available at : https://www.tripwire.com/state-of-security/ics-security/tripwire-visibility-ics/.
16. Сайт SearchInform. Контур Інформаційної Безпеки SearchInform [Електронний ресурс]. — Режим доступу : http://searchinform.com.ua.

References

1. Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011, May). DRAFT Cloud Computing Synopsis and Recommendations. *NIST*. Retrieved from http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf.
2. Challenging Security Requirements for US Government Cloud Computing Adoption (Draft) (2011, November). *NIST*. Retrieved from http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Requirements _for_US_Government_Cloud.pdf.
3. Jansen, W., & Grance, T. (2011, December). Guidelines on Security and Privacy in Public Cloud Computing. *NIST*. Retrieved from https://csrc.nist.gov/publications/ detail/sp/800-144/final.
4. Dodson, D., Carroll, D., Scinta, G., Prafullchandra, H., Singh, H., Yeluri, R., et al. (2018, August). Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments Relevance. *NIST*. Retrieved from https://csrc.nist.gov/publications/detail/sp/1800-19/draft.
5. Site SAP Cloud Platform. (n. d.). *help.sap.com*. Retrieved from https://help.sap.com/viewer/65de2977205c403bbc107264b8eccf4b/Cloud/en-US/eb70f16b420447b6b33dedc3ebcf91cc.html.
6. Site Oracle. (n. d.). Cloud Security Ebook. *www.oracle.com*. Retrieved from https://www.oracle.com/security/index.html.
7. Buldakova, T. I., & Korshunov, A. V. (2015). Obespechenie informacionnoi bezopasnosti ERP-sistem [Ensuring the information security of ERP-systems]. *Voprosy kiberbezopasnosti. Specialnyi vypusk — Cyber security issues. Special issue, 5* (13), 41—44 [in Russian].
8. Catteddu, D., & Hogben, G. (2009). Cloud Computing Benefits, risks and recommendations for information security. *The European Network and Information Security Agency*. Retrieved from https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security.
9. Patel, A., Taghavi, M., Bakhtiyari, K., & Celestino, J. (2013). An Intrusion Detection And Prevention System In Cloud Computing: A Systematic. *Júnior Journal of Network and Computer Applications, 36* (1), 25—41.
10. SAP Cloud Platform. (n. d.). *help.sap.com*. Retrieved from https://help.sap.com/doc/ bd6250c40c9c4c5391e3009a6f26dc3b/Cloud/en-US/SAP_Cloud_Platform.pdf.
11. SAAS Security: Best Practices for Minimizing Risk in the Cloud. (n. d.). Retrieved from https://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/saas-security-best-practices-minimizing-risk-in-the-cloud-paper.html.
12. Sait CNEWS. Ekspertiza REDSYS. U 77% kompanii net avariinogo plana reagirovaniya na kiberataki [Site CNEWS. Expertise REDSYS. 77% of companies do not have an emergency cyber attack plan]. (2018). *redsys.cnews.ru*. Retrieved from http://redsys.cnews.ru/news/top/2018-05-24_u_77_kompanij_net_avarijnogo_plana_reagirovaniya [in Russian].
13. Panorama consulting solutions. 2019 Top 10 Distribution ERP Systems Report. (n. d.). *cdn2.hubspot.net*. Retrieved from https://cdn2.hubspot.net/hubfs/4439340/Top-10-Distribution-ERP-Systems-2.pdf.
14. SAP Help Portal. (n. d.). Protection from Web Attacks. *help.sap.com*. Retrieved from https://help.sap.com/viewer/65de2977205c403bbc107264b8eccf4b/Cloud/en-US/52750a8f86bb428ca224daa4312d122e.html.
15. The State of Security. (n. d.). Tripwire Visibility for ICS: Getting From Data Mountains to Event Nuggets. *www.tripwire.com*. Retrieved from https://www.tripwire.com/state-of-security/ics-security/tripwire-visibility-ics.
16. Sait SearchInform. (n. d.). Kontur Informaciinoi Bezpeky SearchInform [Site SearchInform. Information Security Contour SearchInform]. *searchinform.com.ua*. Retrieved from http://searchinform.com.ua [in Ukrainian].