Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Мінгальова Владислава Євгеновича*

академічної групи *125м-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Засоби забезпечення конфіденційності інформації при використанні віддалених робочих місць на підприємстві*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Сафаров О.О.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Мінгальову Владиславу Євгеновичу* **академічної групи** *125м-20-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Засоби забезпечення конфіденційності при використанні віддалених робочих місць на підприємстві***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.12.2021 №1036-с

Розділ	Зміст	Термін виконання
Розділ 1	Проаналізувати основні загрози при віддаленому режимі роботи підприємства та його інформаційні потоки. Розробити моделі порушника та загроз.	02.11.2021
Розділ 2	Запропонувати програмно-апаратні та організаційні рішення для забезпечення кращого стану захищеності підприємства, розробити інструкції їх конфігурування	22.12.2021
Розділ 3	Провести економічне обґрунтування розробки	08.01.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 02.09.2021 р.

Дата подання до екзаменаційної комісії: 14.01.2022 р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 135 с., 61 рис., 21 табл., 4 додатка, 30 джерел.

Об'єкт дослідження: інформаційна система підприємства.

Мета кваліфікаційної роботи: забезпечення конфіденційності інформації при використанні віддалених робочих місць на підприємстві.

У першому розділі кваліфікаційної роботи проаналізовані основні загрози при віддаленому режимі роботи підприємства та його інформаційні потоки. Також було розроблено моделі порушника та загроз, завдяки чому для підприємства виявлені актуальні загрози.

У другому розділі кваліфікаційної роботи запропоновані програмно-апаратні та організаційні рішення для забезпечення кращого стану захищеності підприємства, розроблені інструкції їх конфігурування. Також обрано стандартний функціональний профіль захищеності, надано опис щодо відповідності ІТС та запропонованих рішень його критеріям та розроблено політики безпеки інформації.

У третьому розділі обґрунтована доцільність запровадження запропонованих в проекті рішень для забезпечення конфіденційності інформації при використанні віддалених робочих місць підприємством, розраховані витрати на розробку політики безпеки, розраховані капітальні та експлуатаційні витрати, оцінені величини збитку від інформаційної атаки на ІТС підприємства та розраховано загальний ефект від впровадження запропонованої системи інформаційної безпеки.

Практичне значення проекту полягає в підвищені рівня захищеності конфіденційності інформації при використанні віддалених робочих місць на підприємстві.

ІНФОРМАЦІЙНА БЕЗПЕКА, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ВРАЗЛИВОСТІ, ПОЛІТИКА БЕЗПЕКИ.

РЕФЕРАТ

Пояснительная записка: 138 стр., 61 рис., 21 табл., 4 приложения, 30 источников.

Объект исследования: информационная система предприятия.

Цель квалификационной работы: обеспечение конфиденциальности информации при использовании удаленных рабочих мест на предприятии.

В первом разделе квалификационной работы проанализированы основные угрозы при удаленном режиме работы предприятия и его информационные потоки. Также были разработаны модели нарушителя и угроз, благодаря чему на предприятии обнаружены актуальные угрозы.

Во втором разделе квалификационной работы предложены программно-аппаратные и организационные решения для обеспечения лучшего состояния защищенности предприятия, разработаны инструкции по их конфигурированию. Также выбран стандартный функциональный профиль защищенности, описано соответствие ИТС и предлагаемых решений его критериям и разработаны политики безопасности информации.

В третьем разделе обоснована целесообразность внедрения предложенных в проекте решений для обеспечения конфиденциальности информации при использовании удаленных рабочих мест предприятием, рассчитаны расходы на разработку политики безопасности, рассчитаны капитальные и эксплуатационные расходы, оценены величины ущерба от информационной атаки на ИТС предприятия и рассчитан общий эффект от внедрения предлагаемой системы информационной сохранности.

Практическое значение проекта заключается в повышении уровня защищенности конфиденциальности информации при использовании удаленных рабочих мест на предприятии.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, МОДЕЛИ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, УЯЗВИМОСТИ ПОЛИТИКА БЕЗОПАСНОСТИ.

ABSTRACT

Explanatory note: 135 p., 61 fig., 21 tab., 4 additions, 30 sources.

Object of research: enterprise information system.

The purpose of the qualification work: to ensure the confidentiality of information when using remote workstations at the enterprise.

The first section of the qualification work analyzes the main threats to the remote mode of work of the enterprise and its information flows. Models of intruders and threats were also developed, thanks to which current threats were identified at the enterprise.

The second section of the qualification work offers software and hardware and organizational solutions to ensure a better state of security of the enterprise, developed instructions for their configuration. A standard functional security profile has also been selected, described how do ITS and the proposed solutions meet its criteria, and information security policies have been developed.

The third section substantiates the feasibility of implementing the proposed solutions to ensure the confidentiality of information when using remote workstations, calculates the cost of security policy development, calculates capital and operating costs, estimates the damage from information attacks on ITS of the enterprise and implementation of the proposed information security system.

The practical significance of the project is to increase the level of protection of information confidentiality when using remote workstations at the enterprise.

INFORMATION SECURITY, THREAT MODEL, VIOLATION MODEL, VULNERABILITIES, SECURITY POLICY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ВМ – віртуальна машина;

ВПЗ - вразливе програмне забезпечення;

ВРМ – віртуальне робоче місце;

Вт – ватт;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

НІП - науково-інженерне підприємство;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

ЦОД – центр обробки даних;

BYOD - Bring Your Own Device;

COVID-19 - Coronavirus Disease 2019;

CRM - Customer Relationship Management;

DHCP - Dynamic Host Configuration Protocol;

DLP – Data Loss Prevention;

DNS - Domain Name System;

HTTP - Hypertext Transfer Protocol;

HTTPS - Hypertext Transfer Protocol Secure;

I/O – Inboard/Outboard;

IP - Internet Protocol;

IPS - Internet Protocol Security;

ISO - International Organization for Standardization;

IT - Information Technology або інформаційні технології;

JSOC - Joint Science Operations Center;

KiB – kibibyte;

LAMP - Linux, Apache, MySQL, PHP/Perl/Python;

MAC - Media Access Control;

MiB – mebibyte;

NAT - Network Address Translation;

PIN - Personal Identification Number;

QEMU - Quick Emulator;

RDP - Remote Desktop Protocol;

SOC - Security Operation Center;

TCP - Transmission Control Protocol;

USB - Universal Serial Bus;

VDI - Virtual Desktop Infrastructure;

VM - Virtual Machine;

VNC - Virtual Network Computing;

VPN - Virtual Private Network.

ЗМІСТ

ВСТУП

Все частіше компаніям доводиться організовувати віддалені робочі місця для своїх фахівців, щоб захистити здоров'я співробітників, оптимізувати робочі процеси та скоротити витрати. Згідно з опитуванням [10], проведеним у березні 2020 р. компанією Gartner, 88% організацій у світі повністю або частково перевели своїх співробітників на дистанційну роботу через пандемію коронавірусу.[5]

Тема поширення коронавірусу знаходиться на піку популярності, злочинці активно використовуватимуть її у фішингових розсилках не тільки на організації, а й на особисті адреси співробітників, їх сторінки в соціальних мережах.

Масовий та спішний перехід компаній на віддалені режими роботи суттєво загострив проблеми інформаційної безпеки. Більшість компаній вперше зіткнулися з таким завданням, тому перехід на віддалений режим роботи викликав у них чимало складнощів.

Компаніям необхідно швидко трансформувати IT-ландшафт, існуючі бізнес-процеси, IT- та ІБ-політики. Але в умовах дефіциту часу не всі приділяли належну увагу питанням безпеки, тож ризики зросли.

Співробітники, які звикли працювати тільки в офісі, не обізнані з питаннями ІБ, є ще більш вразливою ланкою у захисті. Вони допускають виток персональних даних колег, договорів із клієнтами, комерційних пропозицій чи бухгалтерської звітності. [11]

Перед службами IT та ІБ постає складне завдання: як зберегти безперервність бізнесу і не відкрити двері злочинцям до систем, що захищаються.

Щоб допомогти розібратися в цьому питанні, у кваліфікаційній роботі будуть розглянуті основні загрози, які важливо врахувати при переході на режим віддаленої роботи, як до них підготуватись та налаштувати безпечний віддалений доступ.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 У зоні найбільшого ризику – віддалені працівники

Більшість експертів вважаюсь, що віддалені співробітники потрапили до зони найбільшого ризику.

Домашні мережі захищені набагато слабше, ніж мережі організацій, що робить підключені до них комп'ютери джерелом серйозних потенційних проблем. До ризиків інформаційної безпеки, пов'язаних з віддаленою роботою, відносяться модифікація трафіку, перехоплення паролів і конфіденційних даних, а також злом маршрутизаторів і перенаправлення користувачів на шкідливі сайти. При цьому особливої небезпеки набувають атаки з використанням методів соціальної інженерії.

Перехід на віддалений режим роботи породив безліч фішингових атак, оскільки тема актуальна і користувачі охоче переходять за «клікбейтними» шкідливими посиланнями. Для привернення уваги жертви як відправника таких фішингових листів може фігурувати Всесвітня організація охорони здоров'я або інша шанована організація.

Раніше, якщо співробітник допускав промах і траплявся, наприклад, на фішинг, інші системи забезпечення ІБ могли його підстрахувати. При спробі надіслати конфіденційну інформацію могла спрацювати DLP, при спробі отримати доступ до системи міг відпрацювати антивірус або IPS. Окреме питання – отримання доступу до корпоративної мережі – навіть якщо логін та пароль користувача були втрачені, міг бути обмежений доступ із використанням віддаленого підключення. Наразі віддалені підключення дозволені, систем ІБ, які страхують користувача, довкола немає, і відповідальність за інформаційну безпеку лежить повністю на користувачеві. В результаті безпека організації стала ще більше залежати від свідомості та поінформованості у питаннях ІБ її співробітників.

1.2 Витік даних – ризики зросли

Більшість компаній не була готова до переходу на віддалену роботу – у цьому режимі виявилося практично неможливо контролювати дії співробітників. Багато хто з них отримав потенційну можливість безкарно зливати конфіденційні дані, у тому числі з використанням особистої техніки (скріншоти, фотографування екрану або роздрукованих документів на смартфон).

Варто відзначити, що можливості вкрасти дані або вивести їх з компанії були доступні і раніше: всі робочі комп'ютери давно підключені до інтернету, а співробітники використовують у роботі власні смартфони, які ніхто і ніяк не контролює. Однак, при переході на віддалення посилився ризик витоку даних при атаці ззовні – коли співробітник працює зі свого комп'ютера та підчепив вірус на якомусь ненадійному сайті. Це значно спрощує зловмисникам як крадіжку чутливих даних, і проникнення у внутрішню мережу компанії.

З технічного боку дистанційна робота стала проблемою для компаній, які не працювали раніше у такому форматі та переходили на нього поспіхом. Типові помилки – тут не захистили канал віддаленого підключення, там не налаштували двофакторну автентифікацію, тут роздали надлишкові доступи до корпоративних ресурсів. У результаті трафік віддалених сесій могли перехопити зловмисники, а співробітники отримати у розпорядження конфіденційні дані, працювати з якими їм не належить. Також, не всім вистачало потужностей, щоб підтримати стабільну роботу корпоративних ресурсів при масі віддалених підключень.

Робота працівників з дому пов'язана з відсутністю достатнього контролю, чим провокує більшу кількість ризиків щодо інформаційної безпеки. Через те, що здебільшого перехід на віддалення був екстрений — більшість сервісів просто фізично не встигли нормально налаштувати.

Компрометація секретів компанії за рахунок витоку важливої, критичної чи конфіденційної інформації – це найбільш небезпечна загроза для організації під час переведення працівників на віддалену роботу:

Організації різко наростили парк ноутбуків для роботи працівників ну віддаленому режимі. Ноутбук є популярним засобом для роботи в такому режимі, однак разом з ноутбуком межу контрольованої зони організації перетинає велика кількість бізнес-критичної інформації, при цьому така інформація напевно активно оброблятиметься в недовіреному середовищі домашніх мереж або публічних точок доступу. Безперечно, переважна більшість сценаріїв реалізації загроз мають схожий результат – дані викрадені або цілісність даних порушена.

1.3 Безпека особистих робочих станцій працівників

Варто також відзначити ймовірність витоків даних і поширення шкідливого ПЗ, оскільки багато співробітників підключаються до мережі організації з використанням особистих ПК. У період карантину захист особистих пристроїв співробітників став актуальним як ніколи раніше.

Центр моніторингу та реагування на кіберзагрози Solar JSOC щодня фіксує пов'язані з цим інциденти: це і розповсюдження шкідливого ПЗ в момент підключення зараженого комп'ютера співробітника до інфраструктури компанії, і компрометація облікових даних віддалених співробітників, та спроби розкрадання конфіденційної інформації внутрішніми.

Замість захищених офісних робочих місць люди тепер використовують свої домашні комп'ютери, на яких не застосовується весь спектр корпоративних засобів захисту. жодної відповідальності за свої дії перед компанією.

Домашній ПК співробітника може бути не захищений навіть антивірусом і немає гарантії, що підхоплений шифрувальник не перекинеться на корпоративну мережу. До того ж удома співробітник сам забуває про безпеку. На роботі його стримують рамки, він пам'ятає, що його роботодавець контролює. Вдома – волі значно більше.

У домашній обстановці люди можуть ставати менш пильними. Персональний комп'ютер використовується для виконання робочих та

особистих завдань одночасно, вкладки з конфіденційною інформацією часто залишаються незакритими, що збільшує ризик випадкових витоків інформації.

Багато адміністраторів інформаційних систем теж перейшли на віддалену роботу і стали виконувати свої функції з домашніх комп'ютерів. А якщо поточні дії над критичним сервісом для бізнесу робить не системний адміністратор, а його дитина? Бізнесу дуже дорого може обійтися така віддалена помилкова дія – тому додатковий рубіж у вигляді контролю дій користувачів став дуже актуальним.

Ще один небезпечний варіант - персональний комп'ютер зі застарілою операційною системою або піратською версією ОС, яка не оновлюється і що страшніше вже знаходиться в ботнеті. Багато користувачів дома не стежать за оновленням прошивки маршрутизаторів, використовуючи дефолтові паролі і в більшості випадків не використовують ліцензійні антивірусні засоби. Вони ж, як правило, найбільш схильні до фішингових компаній зловмисників з використанням соціальної інженерії.

Як наслідок цього відбуваються витоки інформації та збільшена кількість хакерських атак на віддалених співробітників з подальшим розвитком атаки на внутрішню інфраструктуру багатьох компаній.

Нинішнє становище незвичне як для звичайних співробітників, так і для багатьох IT/ІБ-фахівців. Оскільки ризик атак на мережі компаній через віддалені робочі місця співробітників і особливо через їх особисті пристрої сильно підвищується, то багатьом компаніям доводиться вносити великі зміни до архітектури мереж, нарощувати потужності та вводити додаткові заходи захисту.

1.4 Використання публічних сервісів

Ще один фактор ризику – масове використання публічних хмарних послуг. Далеко не всі компанії придбали комерційні підписки, а використання безкоштовної персональної підписки, що часто не гарантує збереження даних або їх конфіденційність.

Відповідних інцидентів зафіксовано безліч: несанкціоновані підключення до відеоконференцій, виток конфіденційних документів із публічних ресурсів. При цьому важливо пам'ятати, що найуразливішим фактором у будь-якій системі інформаційної безпеки залишається людський. Багато компаній не приділили належної уваги навчанню працівників правилам кібербезпеки при віддаленій роботі. Наслідком цього стало використання тіньових IT-сервісів та незахищеність перед новими хитрощами зловмисників, що з'явилися в період пандемії.

Зокрема, останнім часом реєструються тисячі доменів, що імітують популярну платформу відеозв'язку Zoom, багато з яких шкідливі чи підозрілі.

Нерідко для зручності у співробітників компанії виникають ідеї обміну корпоративною критичною інформацією через хмарні системи, в месенджерах і соцмережах або використання домашнього незахищеного ПЗ для службових цілей.

1.5 Неправильна побудова віддаленого режиму роботи

Поточна ситуація є вкрай складною для співробітників підрозділів IT та ІБ. Навіть ті компанії, які мали можливість віддаленого доступу до корпоративних систем, зіткнулися з необхідністю швидкого переведення великої кількості працівників на віддалену роботу. В наш час існує достатня кількість підходів та засобів захисту інформації, здатних забезпечити повноцінну роботу працівників у віддаленому режимі роботи без суттєвого зростання загроз для корпоративних систем. За наявності достатнього часу та коштів можна побудувати захищену систему віддаленого доступу працівників.

Справа в тому, що цього разу необхідного часу якраз і не було. Більшості компаній довелося перебудовувати свої системи та процеси дуже швидко і при цьому питання безпеки не були перші в пріоритеті. Деякі компанії до введення режиму самоізоляції взагалі не припускали будь-коли використовувати віддалений доступ для повноцінної роботи своїх співробітників. І в цьому випадку їм, звичайно, довелося створювати такі системи буквально на коліні.

Все це призвело до того, що створені та працюючі і в даний час системи віддаленого доступу відповідають далеко не всім вимогам з інформаційної безпеки. І навіть зараз багато компаній не впровадили всі необхідні засоби захисту і не вибудували свої процеси для забезпечення безпечного віддаленого доступу співробітників. Таким чином, найнебезпечнішою є не якась конкретна загроза, а загальний рівень безпеки систем віддаленого доступу, побудованих за короткий термін у прискореному режимі.

При цьому багато компаній не змогли перейти на віддалену роботу зберігши той самий рівень безпеки та контролю дій користувачів, який забезпечували у стандартному режимі роботи.

Близько 11% опитаних респондентів компанією Positive Technologies відзначили, що віддалена робота в їхніх компаніях організовувалась екстрено. IT-інфраструктура перебудовувалась дуже швидко і головним завданням було забезпечити безперебійність роботи критичних бізнес-процесів, а вимоги ІБ нерідко ігнорувалися. Наприклад, на мережевому периметрі компаній різко збільшилася кількість ресурсів, атака на які могла б дозволити зловмисникам отримати контроль над сервером та проникнути в локальну мережу. І пов'язано це було, швидше за все, саме з поспішним переведенням частини співробітників на віддалену роботу.

Одне з досліджень тієї ж компанії показало, що майже п'ята частина організацій, що перейшли на віддалений режим роботи, так чи інакше на своєму периметрі опублікували корпоративні web-портали. При тому раніше вони були доступні лише внутрішнім користувачам, а це означає, що з високою ймовірністю питання їхньої захищеності мало низький пріоритет, тобто не всі вони відповідають вимогам безпеки і не завжди закриті всі вразливості. [7]

Різні тимчасові схеми віддаленого доступу, які вводилися в режимі «зараз потрібно терміново, але потім виправимо», часто зберігаються надовго. Одне з опитувань компанії показало, що у 57% випадків методи організації віддаленого доступу організаціях міняти не планують.

В основному компанії та організації заплющують очі на використання особистих пристроїв у корпоративній мережі, доступ з них до незахищених корпоративних сервісів, встановлення ПЗ за бажанням співробітника, а не на вимогу компанії.

У період епідемії проблеми безпечного доступу із незахищених пристроїв не виникли, а загострилися. Досі не всі усвідомлюють, що відмова від якісного антивірусу, використання безкоштовного урізаного виробу в чомусь схоже на відмову від вакцинації. "Відмовники" мають перевагу: вони отримують на свої комп'ютери дані із захищених пристроїв, їх пристрої працюють без антивіруса швидше, немає обмежень на відвідування нерекомендованих сторінок. Але все руйнується, коли всі починають обмінюватися листами з незахищених пристроїв, у той час як на поштових серверах, що використовуються, теж немає антивірусу з антиспамом.

1.6 Новий периметр захисту

У багатьох компаній вся архітектура безпеки була побудована на основі того, що пристрої, що захищаються, знаходяться в периметрі організації.

Перехід на віддалення дуже сильно розмив цей периметр, у результаті стали актуальними відповідні загрози. До традиційних загроз інформаційній безпеці додалися нові, що ускладнили завдання забезпечення захисту IT-інфраструктури.

Звичне поняття периметра остаточно втратило актуальність, збільшилася різноманітність комп'ютерної техніки, використовуваної співробітниками для роботи у віддаленому режимі роботи, адміністратору стало значно складніше, а іноді й просто неможливо контролювати робочі пристрої користувачів та доступ до них. Тому зросла необхідність оперативного моніторингу та контролю всієї системи захисту інформаційної структури організації, а також застосування перевірених та надійних засобів захисту віддаленого доступу.

Масове переміщення працівників за периметр організації є однією з найнебезпечніших загроз у віддаленому режимі роботи. Співробітники, що

працюють з дому, знаходяться в зоні підвищених ризиків кібербезпеки відразу з кількох причин: відсутність контролю за встановленим ПЗ, шкідливі веб-ресурси, вихід у мережу через незахищені з'єднання, використання власних пристроїв.

Одночасно з переходом на «віддалення» виріс периметр атаки на компанії і підвищилися ризики витоку інформації з неконтрольованих пристроїв користувача.

Все це послужило імпульсом зростання активності зловмисників, які вже промацують компанії в пошуках незахищених систем. При цьому атакуючі найчастіше використовують старі перевірені методи: фішингові розсилки, перебір паролів, пошук відомих уразливостей тощо.

1.7 Загрози після повернення з віддаленого режиму роботи

Ступінь автоматизації проникнення та зараження інфраструктури така, що будь-яка компанія, підключена до інтернету моментально становиться ціллю сотень скриптів і програм, які намагаються заслати шифрувальника, встановити майнер, розширити ботнет, відправити поштою вірус тощо.

Ми в Центрі моніторингу кібербезпеки SOC НІП «Інформзахист» спостерігається понад 4 мільйони спроб проникнень щороку на підконтрольну інфраструктуру. Швидше за все більшість компаній не готувалися до масового переведення співробітників на віддалений режим роботи. І зараз, коли маса співробітників піде зі своїх домашніх комп'ютерів або ноутбуків в інфраструктуру своїх роботодавців, кількість точок потенційного проникнення та зараження зросте на порядки. [7]

Тому довгоочікуваний вихід з режиму віддаленої роботи служб ІБ, адаптованих до нових умов, далеко ще не привід у тому, щоб розслабитися тому, що недостатньо просто відновити ті процеси, які існували раніше. Вихід співробітників до офісів з віддаленої роботи вимагає врахувати низку нових ризиків.

Необхідна перевірка всього обладнання, що повертається в офісну мережу, на наявність шкідливого ПЗ, яке далеко не завжди виявляється стандартними антивірусними засобами. Або, наприклад, після повернення з віддаленого режиму роботи всі без винятку паролі співробітників варто оновити. Периметр компанії тепер інший і вимагає оперативної інвентаризації на предмет сервісів, що доступні з інтернету. Також треба враховувати, що в період тотального видалення зловмисник за бажанням вже мав шанс проникнути в інфраструктуру, тому службам ІБ необхідно провести ретроспективний аналіз і переконатися, що системи не були зламані в період віддаленого режиму роботи або раніше.

1.8 Інформаційні потоки

Для типового підприємства на 8+ співробітників з продажу товарів/послуг у віддаленому режимі роботи будуть актуальними інформаційні потоки, що наведені у таблиці 1.1 та зображені на рисунку 1.1.

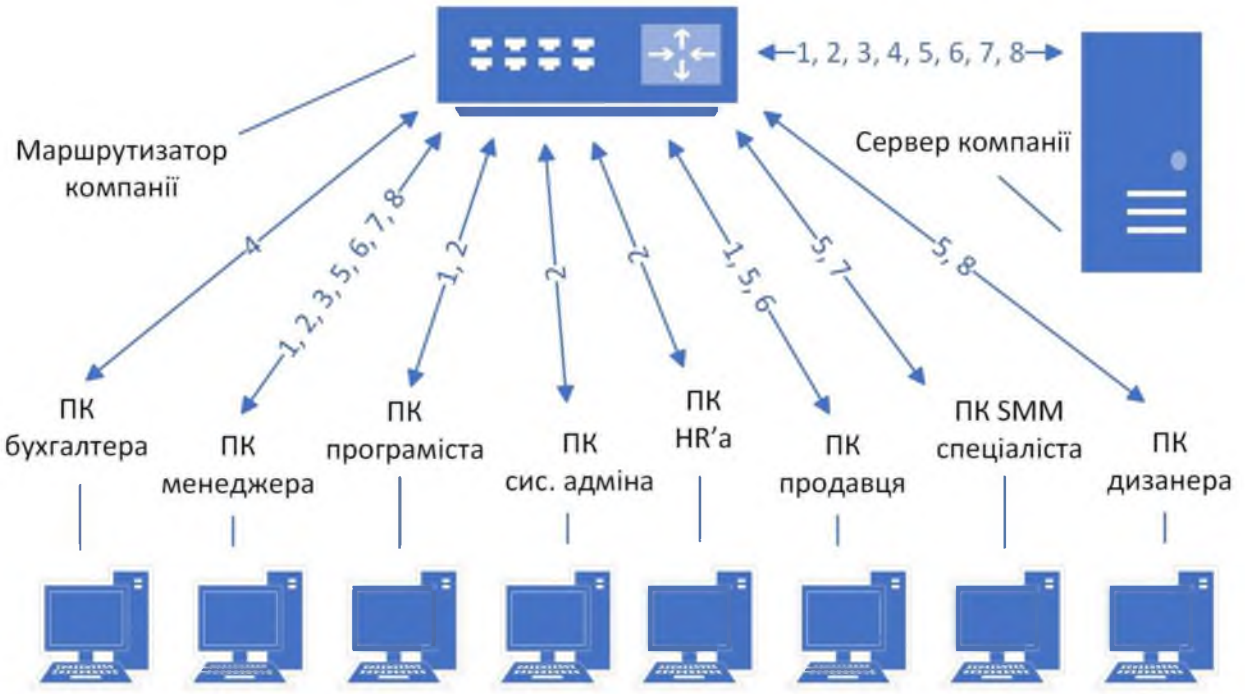


Рисунок 1.1 – Схема інформаційних потоків

Номери зазначених інформаційних потоків наведені у таблиці 1.1

Таблиця 1.1 – Форми подання інформаційних потоків

№	Дані, які обробляються
1.	Персональні дані клієнтів
2.	Персональні дані співробітників
3.	Контракти з клієнтами
4.	Податкові декларації
5.	Інформація про товар
6.	Облік продажів
7.	Рекламна стратегія
8.	Макети дизайну

1.9 Модель порушника

Таблиця 1.2 - Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
Внутрішні по відношенню до ІТС		
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	1
ПВ2	Персонал, який обслуговує технічні засоби ІТС (інженери, техніки)	2
ПВ3	Користувачі (оператори) ІТС	2
ПВ4	Адміністратори ІТС, співробітники служби захисту інформації	3
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	4
Зовнішні по відношенню до ІТС		
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів або закордонних спецслужб «під прикриттям»	4

Таблиця 1.3 - Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов'язок (ПЗ4)	4

Таблиця 1.4 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 1.5 - Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2

Таблиця 1.6 - Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час повної бездіяльності ІТС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІТС (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС, так і під час призупинки компонентів системи	4

Таблиця 1.7 - Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Таблиця 1.8 - Модель порушника політики безпеки інформації

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Загальна сума
Бухгалтер	ПВ3	М3	К2	З1	Ч4	Д3	15
	2	3	2	1	4	3	
	П34	М4	К4	З2	Ч3	Д3	22
	4	4	4	2	3	3	
Менеджер відділу продажів	ПВ3	М3	К2	З1	Ч4	Д3	15
	2	3	2	1	4	3	
	П34	М4	К4	З2	Ч3	Д3	22
	4	4	4	2	3	3	

Продовження таблиці 1.8

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Загальна сума
Програміст 1С	ПВ3	М2	К3	З1	Ч4	Д3	14
	2	2	3	1	4	3	
	П34	М4	К4	З2	Ч3	Д3	22
	4	4	4	2	3	3	
Системний адміністратор	ПВ4	М2	К4	З1	Ч4	Д4	18
	3	2	4	1	4	4	
	П34	М4	К4	З2	Ч3	Д4	23
	4	4	4	2	3	4	
HR	ПВ3	М2	К2	З1	Ч4	Д2	13
	2	2	2	1	4	2	
	П34	М4	К4	З2	Ч3	Д2	21
	4	4	4	2	3	2	
Продавець	ПВ3	М3	К2	З1	Ч4	Д3	15
	2	3	2	1	4	3	
	П34	М4	К4	З2	Ч3	Д3	22
	4	4	4	2	3	3	
SMM спеціаліст	ПВ3	М2	К2	З1	Ч4	Д2	13
	2	2	2	1	4	2	
	П34	М4	К4	З2	Ч3	Д2	21
	4	4	4	2	3	2	
Дизайнер	ПВ3	М2	К2	З1	Ч4	Д2	13
	2	2	2	1	4	2	
	П34	М4	К4	З2	Ч3	Д2	21
	4	4	4	2	3	2	
	4	4	4	2	3	3	

1.10 Модель загроз

1.10.1 Класифікація джерел загроз

Для оброблювальної в ІТС інформації характерними можуть буди наступні джерела загроз:

1. Антропогенні:

1.1 Внутрішні:

1.1.1 Бухгалтер;

1.1.2 Менеджер відділу продажів;

1.1.3 Програміст 1С;

1.1.4 Системний адміністратор;

1.1.5 HR;

1.1.6 Продавець;

1.1.7 SMM спеціаліст;

1.1.8 Дизайнер.

1.2 Зовнішні:

1.2.1 Конкуренти;

1.2.2 Злочинці;

1.2.3 Представники наглядових організацій та аварійних служб.

1.2.4 Родичі

2. Техногенні:

2.1 Внутрішні:

2.1.1 Неякісні технічні засоби обробки інформації;

2.1.2 Неякісне ПЗ обробки інформації.

2.2 Зовнішні

2.2.1 Мережі інженерних комунікацій.

3. Стихійні:

3.1 Пожежа;

3.2 Воєнні дії;

3.2 Інші непередбачені обставини.

Наведені джерела загроз необхідно проранжувати за ступенем небезпеки ($К_{неб}$) скориставшись формулою:

$$(К_{неб})_i = \frac{К1 * К2 * К3}{125} \quad (1.1)$$

де і – джерело загрози;

Кі – критерії порівняння показників.

В якості критеріїв порівняння показників, обрано:

1. Можливість виникнення джерела (К1) – визначає ступінь доступності до об'єкта, віддаленість від об'єкта, особливість обстановки.

2. Готовність джерела (К2) – визначає ступінь кваліфікації порушника та ступінь його мотивації реалізувати загрозу, присутність необхідних умов.

3. Фатальність (К3) – визначає ступінь фатальності наслідків.

Результати обчислень та ранжування загроз за ступенем небезпеки наведено у таблиці 1.9.

Таблиця 1.9 – Ранжування загроз

Джерело загрози	К1	К2	К3	$К_{неб}$
Бухгалтер	4	2	2	0.16
Менеджер відділу продажів	4	2	3	0.24
Програміст 1С	4	3	3	0.288
Системний адміністратор	4	4	3	0.48
HR	4	2	2	0.16
Продавець	4	2	3	0.24
SMM спеціаліст	4	2	2	0.16
Дизайнер	4	2	2	0.16
Конкуренти	2	1	1	0.016

Продовження таблиці 1.9

Джерело загрози	К1	К2	К3	$К_{неб}$
Злочинці	2	1	3	0.05
Представники наглядових організацій та аварійних служб	2	1	1	0.016
Родичі	2	1	1	0.016
Неякісні технічні засоби обробки інформації (сервер, ПК)	4	3	3	0.36
Неякісне ПЗ обробки інформації	4	3	3	0.36
Пожежа	2	3	4	0.192
Воєнні дії	1	1	4	0.016
Мережі інженерних комунікацій	4	3	3	0.288
Інші непередбачені обставини	2	3	3	0.144

Кожен з трьох критеріїв оцінюється експертно-аналітичним способом по п’ятибальній шкалі.

К1 для антропогенних:

- 1 – відсутність доступності до об’єкта;
- 2 – низький ступінь доступності до об’єкта;
- 3 – джерело має обмежений доступ до технічних і програмних засобів обробки інформації;
- 4 – джерело має доступ до технічних і програмних засобів обробки інформації, але це не входить в його функціональні обов’язки;
- 5 – джерело має повний доступ до технічних і програмних засобів обробки інформації.

К1 для техногенних:

- 1 - дуже віддалені об’єкти;
- 2 - віддалені об’єкти, але джерело може впливати на них;
- 3 - джерело знаходиться недалеко від ОІД;

– 4 - джерело знаходиться біля ОІД;

– 5 - сам об’єкт містить джерело загроз.

К1 для стихійних:

– 1 - відсутність на ОІД передумов виникнення джерел загроз;

– 2 - є незначні передумови виникнення джерела загрози;

– 3 - відсутність довгого періоду проявів джерела загрози, але наявність передумови до його появи;

– 4 - висока ймовірність появи джерела;

– 5 - об’єкт знаходиться у зоні прояву джерела.

К2 для антропогенних:

– 1 – відсутність можливості використання будь-яких програм;

– 2 – запуск фіксованого набору програм;

– 3 – створення та запуск власних програм з новими функціями обробки інформації;

– 4 – можливість впливати на базове ПЗ;

– 5 – весь обсяг можливостей суб’єкта (створення власних технічних засобів з новими функціями обробки інформації).

К2 для техногенних:

– 1 - інформація не являє інтерес для джерела;

– 2 -накопичувана інформація, яка після розголошення може принести збитки ОІД;

– 3 - інформація, яка може принести збитки окремим особам;

– 4 - інформація, яка може принести вигоду джерелу загрози або третім особам;

– 5 - інформація, яка може привести до непоправної шкоди та до краху ОІД.

К2 для стихійних:

– 1 - відсутні передумови для реалізації джерела загрози;

– 2 - наявність умов на об’єкті, що запобігають прояву джерела загрози;

– 3 - сприятливі умови для реалізації загрози, але мала вірогідність прояву джерела;

– 4 - сприятливі умови для прояву джерела загроз;

– 5 - сприятливі умови для прояву джерела загроз.

КЗ:

– 1 – загроза ніяк не вплине на ОІД;

– 2 – незначні наслідки, які не потребують великих затрат;

– 3 – відчутні наслідки, які потребують затрати;

– 4 – наслідки, які потребують значних матеріальних та часових затрат;

– 5 – майже незворотні наслідки.

Джерела загроз, у яких $К_{неб}$ менше 0.17, надалі не розглядаються вважаючись маловірогідними.

1.10.2 Класифікація вразливостей

Джерела загроз можуть використовувати вразливості для порушення безпеки інформації. Проаналізувавши ОІД, можемо навести наступні вразливості ІТС:

1. Суб’єктивні:

1.1 Відсутність відеоспостереження;

1.2 Недосвідченість персоналу з питань ІБ;

1.3 Розповсюдження працівниками ІзОД;

1.4 Несвоєчасне оновлення ПЗ;

1.5 Відсутність розмежування доступу до інформації;

1.6 Відсутність контролю за WEB-трафіком;

1.7 Використання неякісного ПЗ.

2. Об’єктивні:

2.1 Незахищений канал передачі даних.

3. Випадкові:

3.1 Збій або відмова технічних засобів;

3.2 Збій або відмова програмного забезпечення;

3.3 Збій електроживлення.

Вразливості, як і джерела загроз, мають різні ступені небезпеки($К_{неб}$), які можливо кількісно оцінити за допомогою ранжування. В якості критеріїв порівняння показників, обрано:

1. Фатальність (К1) – ступінь фатальності наслідків.

2. Доступність (К2) – можливість використання вразливості джерелом загрози.

3. Кількість (К3) – кількість елементів об’єкту, яким характерна вразливість.

Тепер проводимо ранжування джерел загроз по ступеню небезпеки користуючись формулою (1.1). Результати наведено у таблиці 1.10.

Таблиця 1.10 – Ранжування вразливостей

Вразливість	К1	К2	К3	$К_{неб}$
Відсутність відеоспостереження	4	3	1	0.096
Недосвідченість персоналу з питань ІБ	2	5	3	0.24
Розповсюдження працівниками ІзОД	3	5	2	0.24
Несвоєчасне оновлення ПЗ	2	3	3	0.14
Відсутність розмежування доступу до інформації	3	3	3	0.216
Відсутність контролю за WEB-трафіком	3	3	3	0.216
Використання неякісного ПЗ.	2	3	3	0.14
Незахищений канал передачі даних	3	4	2	0.192
Збій або відмова технічних засобів	2	3	3	0.14
Збій або відмова програмного забезпечення	2	3	3	0.14
Збій електроживлення	2	3	1	0.05

Кожен з трьох критеріїв оцінюється експертно-аналітичним способом по п’ятибальній шкалі.

К1:

- 1 – підприємство не понесе значних втрат;
- 2 – мала ймовірність реалізації загрози;
- 3 – може призвести до реалізації загрози;
- 4 – висока ймовірність реалізації загрози;
- 5 – загроза буде реалізована.

К2:

- 1 – вразливістю майже неможливо скористатися;
- 2 – щоб скористатися вразливістю необхідно витратити багато ресурсів;
- 3 – вразливістю можна скористатися за певних умов;
- 4 – щоб скористатися вразливістю необхідно мати певні навички;
- 5 – вразливістю може скористатися будь-яка людина.

К3:

- 1 – Вразливість притаманна одному елементу;
- 2 – Вразливість притаманна 2 – 10 елементам;
- 3 – Вразливість притаманна 11 – 16 елементам;
- 4 – Вразливість притаманна 17 – 22 елементам;
- 5 – Вразливість притаманна більше ніж 23 елементам.

Вразливості, у яких $К_{неб}$ менше 0.17, надалі не розглядаються вважаючись маловірогідними.

1.10.3 Класифікація актуальних загроз

Далі в таблиці 1.11 наведена матриця взаємозв’язку джерел загроз та вразливостей, та коефіцієнт небезпеки цих атак.

Таблиця 1.11 Матриця загроз

Джерела загроз	Вразливості				
	Недосвідченість персоналу з питань ІБ	Розповсюдження працівниками ІзОД	Незахищений канал передачі даних	Відсутність розмежування доступу до інформації	Відсутність контролю за WEB-трафіком
Менеджер відділу продажів	0.057	0.057	0.046	0.051	0.051
Продавець	0.057	0.057	0.046	0.051	0.051
Системний адміністратор	0.115	0.115	0.092	0.103	0.103
Програміст 1С	0.069	0.077	0.069	0.077	0.077
Неякісні технічні засоби обробки інформації (сервер, ПК)	0.086	-	-	-	0,077
Неякісне ПЗ обробки інформації	0.086	-	-	-	0,077

Загрози, що мають коефіцієнт менше 0.8, можуть надалі не братись до уваги, як маловірогідні. Після аналізу матриці, актуальними загрозами є:

– Викрадення, знищення або пошкодження інформації системним адміністратором через погану комп'ютерну обізнаність персоналу та розповсюдження ними ІзОД, відсутності паролів на ноутбуках. Можливий мотив - корисливий інтерес.

– Втрата доступності до інформації або повне її знищення на сервері, у результаті відсутність контролю за встановленням та оновленням ПЗ.

У таблиці 1.12 наведена класифікація загрози за її впливом на властивості інформації: К – конфіденційність, Ц – цілісність, Д – доступність.

Таблиця 1.12 Класифікація загроз за впливом на властивості інформації

Загрози	Які властивості інформації порушуються		
	К	Ц	Д
Викрадення, знищення або модифікація ІзОД системним адміністратором	+	-	-
Знищення ІзОД через збій у роботі засобів обробки інформації, на яких вона зберігається	-	-	+
Пошкодження ІзОД або унеможливлення доступу до неї через використання неякісного ПЗ	-	-	+

1.11 Висновки

У першому розділі кваліфікаційної роботи було проведено аналіз основних загроз при віддаленому режимі роботи підприємства, його інформаційні потоки, розроблено модель порушника та модель загроз, за допомогою яких виявлено актуальні загрози для підприємства.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Безпека робочого місця

Потрібно зрозуміти, як здійснюватиметься робота співробітника з дому — на корпоративному ноутбуці, принесеному з офісу на робочому комп'ютері або через віддалене підключення до мережі організації з особистого пристрою (концепція BYOD). Від цього залежать заходи безпеки, які варто передбачити.

Люди часто працюють із дому на власних комп'ютерах. Контролювати, яке на них встановлено програмне забезпечення, неможливо. Часто на домашніх пристроях відсутній антивірус, може стояти Windows XP, завантажений з торенту, троянські програми тощо. Коли цей комп'ютер використовується для доступу в робочий простір, конфіденційна інформація може витекти.

Найбезпечнішим варіантом можна вважати роботу на корпоративному пристрої. Для нього можна заздалегідь забезпечити виконання всіх вимог організації до безпеки віддаленого робочого місця (наприклад, встановити корпоративний антивірус, необхідний для роботи програмного забезпечення, забезпечити двофакторну автентифікацію, шифрування диска, належний рівень журналу подій, а також своєчасне автоматичне оновлення всіх систем). У випадку з особистим пристроєм такі заходи організувати складно, а контролювати їхнє дотримання практично неможливо. З'являється загроза компрометації особистого пристрою працівника внаслідок зараження шкідливим програмним забезпеченням або розкрадання облікового запису внаслідок фішингової атаки.

Якщо організації почнуть дозволяти працівникам використовувати власні ноутбуки безконтрольно, загроза проникнення порушника в мережу організації стане як ніколи актуальною. Необхідно заборонити підключення з таких пристроїв, якщо на них відсутня антивірусний захист і не встановлені всі актуальні оновлення для ПЗ і ОС.

Якщо особистий пристрій співробітника не задовольняє умови для безпечної віддаленої роботи, вирішити проблему з небезпечними домашніми станціями можна, надавши йому корпоративну робочу станцію, наприклад, ноутбук або бездискову робочу станцію, які будуть розглянуті нижче.

2.1.1 Ноутбук

Ноутбуком називають переносний комп'ютер, у корпусі якого об'єднані типові компоненти ПК, включаючи дисплей, клавіатуру та пристрій вказівки (зазвичай сенсорна панель або тачпад), а також акумуляторні батареї. Ноутбуки відрізняються невеликими розмірами та вагою, час автономної роботи ноутбуків варіюється в межах від 1 до 20 годин. Приклад того, як виглядає типовий ноутбук зображено на рисунку 2.1.

Рисунок 2.1 – Ноутбук [29]

Портативні комп'ютери здатні виконувати ті самі завдання, що й настільні комп'ютери, хоча при рівній ціні, продуктивність ноутбука буде істотно нижчою. Ноутбуки містять компоненти, подібні до тих, які встановлені в настільних комп'ютерах, і виконують ті ж самі функції, але мініатюризовані та оптимізовані для мобільного використання та ефективної витрати енергії. Переваги та недоліки ноутбуків наведено у таблиці 2.1.

Таблиця 2.1 – Переваги та недоліки ноутбуків

Переваги	- Мала вага та габарити. Ноутбук можна взяти для віддаленого режиму роботи; - для роботи не обов'язково підключати зовнішні пристрої. Ноутбук включає вбудовані дисплей, клавіатуру та пристрій вказівки (зазвичай тачпад); - можливість автономної роботи. Наявність акумулятора дозволяє ноутбуку працювати в умовах, коли електрична мережа недоступна (у поїзді, літаку, автомобілі, кафе та просто на вулиці); - можливість підключення до бездротової мережі. Майже всі сучасні ноутбуки оснащені вбудованим Wi-Fi адаптером, що дозволяє підключитися до інтернету без дротів.
Недоліки	- Низька максимальна продуктивність. Компактні розміри ноутбуків пред'являють особливі вимоги до охолодження, тому компоненти, що використовуються в ноутбуках, мають жорсткі обмеження з тепловиділення, а отже, і потужності. Тому в ноутбуках встановлюються не продуктивні настільні процесори і використовуються мобільні версії відеокарт; - попадання рідини та конденсат. Різке нагрівання внутрішніх частин холодного ноутбука, принесеного з морозу, призводить до утворення конденсату всередині корпусу, короткого замикання і, відповідно, несправностей. Той самий ефект дає рідина, пролита на клавіатуру; - підвищена ймовірність поломки. Мобільність ноутбуків породжує ще одну проблему - більша ймовірність поломки. Ноутбуки частіше кидають. Якщо залити клавіатуру ноутбука будь-якою рідиною, то велика можливість виходу портативного комп'ютера з ладу; - засмічення клавіатури. Від мобільності ноутбуків також страждає клавіатура. Щоб уникнути ефекту «залипання», потрібно періодично проводити профілактичне чищення або продув клавіатури. [9]

2.1.2 Бездискова робоча станція

Бездискова робоча станція — це персональний комп'ютер, позбавлений незнімних засобів довгострокового зберігання даних.

Існують два основні сценарії використання бездискових робочих станцій:

- товстий клієнт - це робоча станція або ПК, які функціонують на основі своєї ОС та наповнені повноцінним набором програмного забезпечення для необхідних завдань користувача. Операційна система та програми завантажуються по мережі з сервера і потім виконуються локально на робочій станції. Результати роботи (наприклад, документи, з якими працює користувач) зберігаються також на сервері або на будь-якому знімному пристрої. Замість сервера для завантаження робочої станції може використовуватися знімний носій, такий як компакт-диск або Flash-накопичувач; [6]

- тонкий клієнт - це спеціалізований міні-ПК з достатніми характеристиками, щоб підтримувати роботу протоколів передачі даних. Операційна система та програми виконуються на сервері, а результати їх роботи (інтерфейс додатків) передаються на робочу станцію і відображаються так само, як якщо б користувач працював з цими програмами безпосередньо. Такі робочі станції називаються терміналами, а сервери, на яких виконуються ОС та програми - серверами терміналів. Термінали вимагають мінімальної обчислювальної потужності, оскільки вони не обробляють дані (нічого не зберігає, не проводить обчислення, не малює графіку), лише транслює зображення з сервера на монітор. З іншого боку, потрібна підвищена продуктивність серверів терміналів. Приклад того, як виглядає типова бездискова робоча станція зображено на рисунку 2.2.

Рисунок 2.2 - Бездискова робоча станція [8]

Інакше кажучи, бездискова робоча станція - це невелика коробка, яку встановлено полегшена ОС, а базове відмінність товстого клієнта від тонкого – це спосіб обробки даних. [13] До основних цілей бездискової робочої станції можна віднести:

- інструмент для зручного оновлення ОС;
- відокремлення операційної системи від обладнання;
- централізація даних користувачів у центрі обробки даних
- інструмент для управління ПЗ, яке доступне користувачам.

Централізоване зберігання всіх даних дозволяє легко керувати ними, виробляти резервне копіювання тощо. З іншого боку, якщо бездискова станція завантажується з сервера або є терміналом, вона непрацездатна без справного мережного підключення і сервера.

Основна маса рішень на користь використання бездискових станцій приймається IT-персоналом з економічної сторони поставленого завдання, оскільки апаратні вимоги зазвичай низькі. Більшість великих виробників серверних рішень виробляють клієнти на сучасних, але низькопродуктивних комплектуючих, через що вони, як правило, споживають набагато менше електрики - 7-15 Вт [11], залежно від моделі.

У клієнта міцний корпус, відсутні рухомі частини, найчастіше немає охолодження та жорсткого диска. Як наслідок, у разі його поломки дані користувача не втрачаються. Він підтримує більшість сучасних інтерфейсів, стійкий до перепадів температури, вологості, що дозволяє збільшити термін його роботи. [11]

Також у бездискової робочої станції існую проблема свопінгу. Підкачування сторінок (також свопінг, від англ. swap) — один з механізмів віртуальної пам'яті, при якому окремі фрагменти оперативної пам'яті переміщуються на жорсткий диск, звільняючи місце біля оперативної пам'яті для завантаження інших фрагментів. [12] У разі бездискового комп'ютера виникають проблеми при розміщенні своп-файлу, оскільки відсутній накопичувач, на якому його зазвичай розміщують. Можуть використовуватися

ОС та оточення, що не вимагають наявності своп-файлу, або своп файл розміщується на сервері. Іноді бездискові станції все-таки забезпечують жорсткий диск невеликої ємності для розміщення тільки своп-файлу. [6] Переваги та недоліки бездискових робочих станцій наведено у таблиці 2.2.

Таблиця 2.2 - Переваги та недоліки бездискових робочих станцій

	Переваги	Недоліки
Товстий клієнт	- велика функціональність; - наявність розрахованого на багато користувачів режиму; - можливість роботи в режимі офлайн; - миттєва швидкодія; – Мінімальна залежність від складних серверів.	- всі робочі машини на постійній основі потребують технічного обслуговування; - потреба в індивідуальному оновленні апаратного ПЗ кожного клієнта до рівня програмного забезпечення, яке використовуватиметься; - масивні обсяги дистрибутивів; - Повна залежність від платформ, під якими дані клієнти були створені.
Тонкий клієнт	- мінімальне апаратне обслуговування; - низький ризик виникнення несправності; - Мінімальні технічні вимоги до апаратного обладнання.	- під час збою на сервері "постраждають" всі підключені користувачі; - немає можливості працювати без активного підключення до мережі; - при взаємодії з великим масивом даних може знижуватись обсяг продуктивності основного сервера.

2.2 Безпека мережевого периметра при клієнт-серверному підключенні

З клієнт-серверним підключенням можна організувати доступ до робочого місця безпосередньо, не через сервери сторонньої організації. Безпека клієнт-серверного підключення залежить від того, як налаштовано контроль доступу. Основні варіанти підключень:

- Відкритий доступ до сервера та терміналів
- Доступ по IP
- Доступ за VPN

2.2.1 Відкритий доступ до сервера та терміналу

Найшвидший спосіб налаштувати клієнт-серверне підключення – зробити відкритий доступ до терміналу та робочих місць. Будь-який комп'ютер може підключитися до сервера і працювати з ним так, начебто знаходиться в офісі.

Відкритий доступ до сервера є небезпечним. В інтернеті лише близько 4 млр. пристроїв [3], а активному стані — ще менше. Щоб просканувати мережу по всіх можливих портах протоколів, достатньо двох місяців. Якщо зловмисник сканує мережу не з одного, а з десятків чи сотень пристроїв, час зменшується у кілька разів.

І якщо до інфраструктури відкрито доступ, за загальновідомим портом rdp tcp/3389, зловмисники можуть виконати довільний код на стороні сервера. За останні кілька років у протоколі RDP кілька разів знаходили вразливості, які дозволяють це зробити.

2.2.2 Доступ через IP

Є кілька варіантів організувати безпечний доступ до серверів компанії:

- Доступ за списком IP-адрес співробітників. Для його організації можна придбати для співробітників статичну IP-адресу або налаштувати підключення за адресами підмережі домашнього оператора. Атаку на ваш сервер можуть провести тільки з підмережі конкретного співробітника – це вже набагато краще, ніж коли двері відчинено усьому інтернету.

- Доступ за динамічним списком (Port Knocking). Це динамічний доступ, що базується на діях співробітників. Можна написати скрипт, який буде робити послідовні дії, щоб отримати доступ до нашої системи. Наприклад: "пропінгувати IP-адресу три рази, потім - з іншим розміром пакета, потім постукати на інший порт - після цього відкриється доступ".

2.2.3 Доступ через VPN

Найбільш актуальні всім компаній у режимі віддаленої роботи стали рішення захисту каналів зв'язку, якими відбувається обмін інформацією. В основі цих рішень – програмні та програмно-апаратні VPN-продукти. Якщо раніше у віддаленому режимі працювали переважно лише співробітники IT-підрозділів, то в період карантинних заходів до них приєдналися й інші фахівці.

VPN - це віртуальна приватна мережа, яку організують технічні спеціалісти. Технологій VPN досить багато. Вибір VPN-рішення залежить від того, що важливіше для компанії: продуктивність, ціна або універсальність.

Причому, за заявами керівників багатьох підприємств, робота у віддаленому режимі виявилася зручною для їх колективів, і вони планують повністю або частково використати цей формат надалі. При такому підході пред'являються більш серйозні вимоги до характеристик користувача VPN-продуктів, а також до якості управління ними. Необхідно, щоб користувач міг легко отримати доступ у корпоративну мережу з будь-якого пристрою та під час використання будь-якої операційної системи, а адміністратор завжди розумів стан цього пристрою.

VPN-тунелювання у поєднанні з налаштованою матрицею доступу дозволило багатьом компаніям швидко перейти на віддалений режим роботи, зберігши розмежування прав доступу до корпоративних інформаційних систем.

Організація VPN-доступу може бути пов'язана з різними проблемами. Зазвичай VPN проводиться до певного мережного сегмента локальної мережі, а доступність інших сегментів у цьому разі не гарантована. IT-підрозділ може просто не встигнути в короткий термін переналаштувати обладнання та забезпечити всіх користувачів VPN необхідним саме їм доступом, не порушуючи правила розмежування. В результаті для забезпечення безперервності бізнесу IT-фахівцям доведеться вибрати найшвидший і найпростіший варіант - відкрити доступ у необхідну підмережу не одному співробітнику, а одразу всім користувачам VPN. Такий підхід суттєво знижує безпеку та відкриває можливості не тільки для атак зовнішнього зловмисника, у

випадку проникнення, але й суттєво підвищує ризик атаки з боку інсайдера. Необхідно приділити особливу увагу моніторингу таких підключень, адже атаки через довірені канали — один із найімовірніших способів проникнення у мережі великих корпорацій.

2.3 Безпека облікових записів

Результати тестувань на проникнення показують [2], що словникові паролі застосовуються як мінімум у 75% компаній для доступу до різних зовнішніх сервісів (зокрема до веб-сайтів, порталів, баз даних, систем телеконференцій). Небезпека значно підвищується, коли слабкі паролі використовуються для віддаленого підключення до локальної мережі. Адже зловмисники можуть підібрати обліковий запис та безпосередньо атакувати внутрішні ресурси.

Вкрай важливо підвищити строгість парольної політики в період віддаленої роботи, як мінімум у частині довжини та складності паролів. Необхідно для віддаленого підключення використовувати паролі довжиною не менше 10 символів для непривілейованих облікових записів та не менше 16 символів для адміністративних. Слід використовувати одночасно різні типи символів (малі та великі літери, спецсимволи, цифри) і виключити використання паролів, що легко вгадуються. Наприклад, у рамках тестувань на проникнення фінансових організацій у 2019 році 48% усіх підібраних паролів було складено з комбінації слова, що позначає пору року або місяць, та чотирьох цифр, що позначають рік (Вересень2019 або в англійській розкладці клавіатури Ctynz,hm2019). Такі паролі підбираються за словниками за лічені хвилини, хоч формально відповідають парольній політиці.

Ризик проникнення в локальну мережу підвищується і за рахунок великої кількості співробітників, яким раніше не надавався віддалений доступ через критичну важливість виконуваних ними завдань. Такі співробітники часто погано навчені тому, як захиститися від кібератаки і яких запобіжних заходів необхідно дотримуватися при роботі в інтернеті. Необхідно бути готовим до

різкого збільшення кількості облікових записів із простими паролями на периметрі мережі. Значне посилення вимог до довжини пароля може стати ефективним заходом з боку IT-департаменту. Перевірити складність паролів також можливо: для цього достатньо вивантажити базу хешей з контролера домену (файл ntds.dit) і спробувати підібрати паролі по цих хешах із застосуванням словників.

Використання двофакторної автентифікації за допомогою апаратних токенів допоможе знизити ризик компрометації мережі компанії у разі підбору словникового пароля працівника. Віддалений доступ підвищує попит на технології багатофакторної автентифікації, що вирішує проблему несанкціонованого доступу до інформації.

2.4 Менеджер паролів

Через велику кількість сервісів з необхідністю реєстрації, якими користуються співробітники, вони часто вдаються до формування нескладних паролів для легкості в їх запам'ятовуванні, навіть якщо вигадують складні паролі, десь їх записують і зберігають у незашифрованому вигляді або просто перевикористовують один і той самий пароль для різних облікових записів, що ставить під загрозу безпеку даних компанії.

Хорошою практикою зберігання та генерації паролів є використання менеджера паролів.

Менеджер паролів — це програмне забезпечення, яке допомагає користувачеві працювати з паролями та PIN-кодами. Таке програмне забезпечення має місцеву базу даних або файли, які містять зашифровані дані пароля. Багато менеджерів паролів також працюють як заповнювач форми, тобто вони заповнюють поле логін і дані пароля автоматично у формах. Зазвичай вони реалізовані як розширення для браузера.

Менеджери паролів поділяються на три основні категорії:

- десктоп - зберігають паролі до програмного забезпечення, встановленого на жорсткому диску комп'ютера;

- портативні - зберігають паролі до програмного забезпечення на мобільних пристроях або до портативних програм на USB-флеш-накопичувачі;

- мережеві - менеджери паролів онлайн, де паролі збережені на веб-сайтах провайдерів.

Менеджери паролів також можуть використовуватися як захист від фішингу. На відміну від людей, програма менеджер паролів може поводитися з автоматизованим скриптом логіна несприйнятливо до візуальних імітацій, які схожі на веб-сайти, тобто, перейшовши за сумнівним посиланням на фішинговий сайт менеджер паролів не підставить логін-пароль у форми введення, а користувач зрозуміє, що сайт є підробкою. З цією вбудованою перевагою використання менеджера паролів вигідно, навіть якщо у користувача є кілька паролів, які він пам'ятає. Проте не всі менеджери паролів можуть автоматично поводитися з більш складними процедурами ідентифікації, накладеними багатьма банківськими веб-сайтами.

Менеджери паролів також маюсь недоліки. Вони зазвичай використовують вибраний користувачем основний пароль, або секретну фразу (passphrase), щоб сформувати ключ, використовуваний для зашифровування паролів, що зберігаються. Цей основний пароль повинен бути досить складним, щоб устояти під час атак зловмисників.

Якщо основний пароль буде зламаний, то будуть розкриті всі паролі, що зберігаються в базі даних програми. Це демонструє зворотний зв'язок між зручністю використання та безпекою: єдиний пароль може бути зручніший, але якщо він буде зламаний, то поставить під загрозу всі паролі, що зберігаються.

Основний пароль може бути атакований при використанні кейлоггера або акустичного криптоаналізу. Така загроза може бути знижена шляхом використання віртуальної клавіатури, наприклад, KeePass.

Деякі менеджери паролів включають генератор паролів. Згенеровані паролі можуть бути відгадуваними, якщо менеджер пароля не використовує криптографічно безпечний генератор випадкових чисел.[14]

Також не найкращим рішенням буде використання вбудованого в браузер менеджера паролів, оскільки вони можуть зберігати записи паролів у незашифрованому вигляді у своїй директорії, що може стати легкою наживою для зловмисника у випадку, якщо він отримав доступ до робочої станції.

Одним з кращих рішень є менеджер паролів Dashlane, який надає безкоштовну версію, що включає:

- сховище для 50 паролів;
- персоналізовані оповіщення безпеки;
- перевірка надійності пароля;
- генератор паролів;
- автозаповнення форм авторизації. [16]

Також Dashline сканує темну мережу на предмет витоку паролів і відправляє користувачеві персоналізовані оповіщення, якщо дані утекли в мережу або були вкрадені. [15]

Dashline підтримує платформи MacOS, Windows, Linux, iOS, Android та плагіни для браузерів Safari, Edge, Google Chrome, Firefox, Internet Explorer. [16]

2.5 Модель захисту нульової довіри

Компаніям необхідно не лише забезпечити шифрування каналу віддаленого підключення. Як ніколи раніше стає актуальною модель захисту нульової довіри (zero trust). Вона передбачає створення підходів до захисту, ґрунтуючись на повній відсутності довіри до будь-яких користувачів, що підключаються до корпоративних ресурсів. Користувачі та пристрої повинні кожного разу підтверджувати свою автентичність під час підключення до ресурсів. Ідея Zero Trust у тому, що для користувачів немає прямих перешкод доступу до системи, але система максимально безпечна.

Приклад Zero Trust – онлайн банкінг. У нього вбудований власний захист: система слідкує за кількістю спроб входу, моніторить уразливості, відстежує

атаки. Користувачі отримують доступ до інформації без додаткових засобів, відокремлених від інформаційної системи.

Ця модель добре корелює з тим, що тепер співробітники підключаються до мережі компанії з будь-якого місця, зокрема з персональних пристроїв. Контроль за цими пристроями за замовчуванням практично відсутній, а отже, довіряти їм неможливо. Хорошою практикою при побудові системи захисту буде прийняти для себе правило, що всі пристрої апріорі можуть бути зламані. При побудові системи захисту компаніям необхідно застосовувати рішення та технології, які забезпечують реалізацію принципів zero trust: багатофакторна автентифікація, що дозволяє захиститись від скомпрометованих паролів співробітників; перевірки пристроїв працівників на наявність встановлених оновлень, актуальність антивірусних баз, захист даних на пристроях співробітників (шифрування) тощо.

Для невеликого корпоративного клієнта Zero Trust може включати двофакторну авторизацію, концепцію захисту від підбору паролів, обов'язкові сертифікати, регулярну перевірку на вразливість.

2.6 Кібергігієна

Продовжується зростання атак, що експлуатують тему коронавірусу: до 13% від усіх атак у першому кварталі були так чи інакше пов'язані з ним. До них увійшли як атаки, що експлуатують тему коронавірусу у фішингових листах, так і атаки на лікарні, які проводять тестування або лікування від коронавірусу. Зловмисники активно використовують електронну пошту для розповсюдження фішингових посилань та шкідливих програм у додатках. І ефективність їх досить висока, оскільки користувачі, отримуючи і цілком легальні розсилки новин про коронавірус, не завжди в загальному їх обсязі можуть розпізнати щось шкідливе. І поки кількість заражених тільки зростає, спектр таких загроз також лише зростатиме. [7]

Злочинці використовують тему пандемії та розсилають фішингові листи з текстом про захист від коронавірусу, створюють фейкові сайти,

розповсюджують трояни під виглядом мобільних додатків. Кіберзлочинці швидко влаштувалися під перехід компаній на віддалену роботу та атакують особисті електронні адреси співробітників. Приклади фішингових повідомлень зображено на рисунках 2.3 та 2.4.

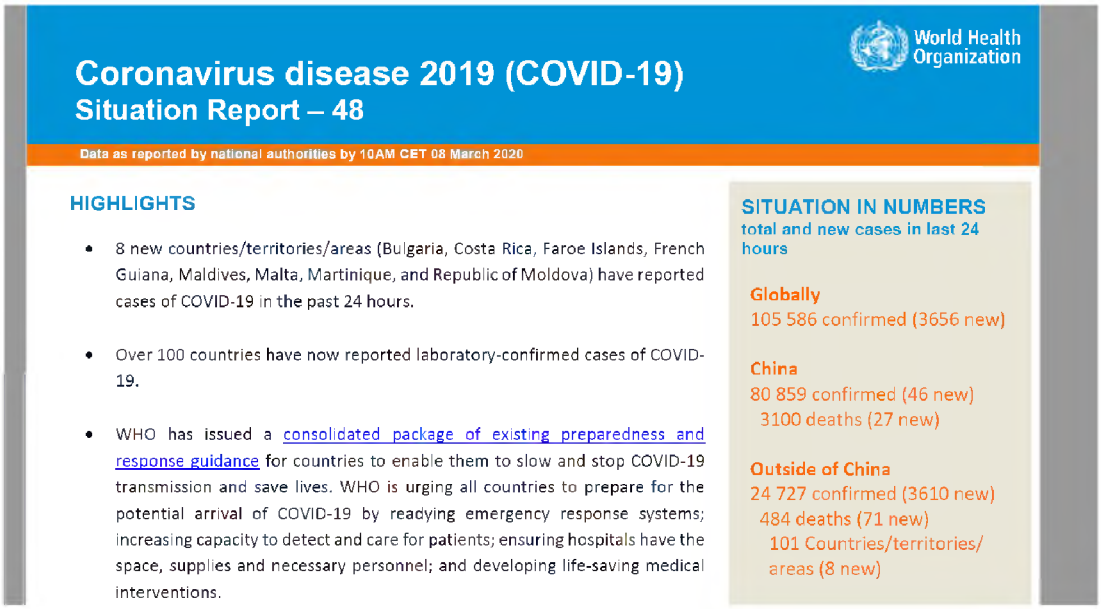


Рисунок 2.3 – Фішингове повідомлення ніби від World Health Organization

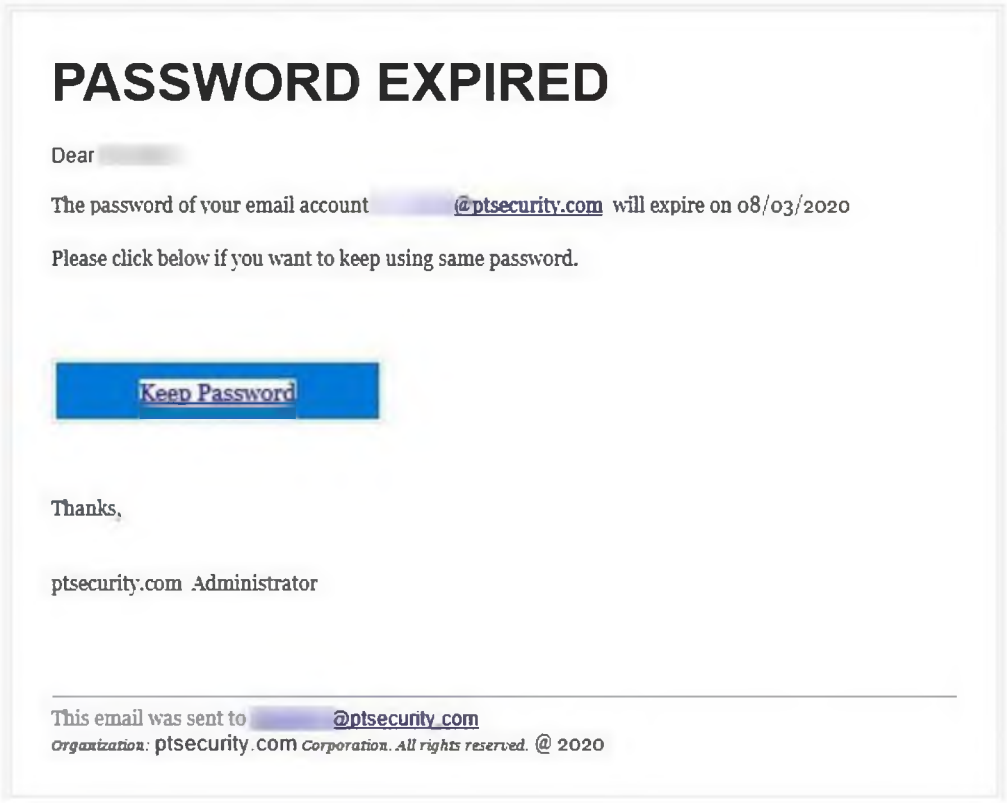


Рисунок 2.4 – Фішингове повідомлення начебто від адміністратора де працює користувач

Співробітники повинні розуміти серйозність загрози та бути готовими відрізнити легітимну пошту від фішингу. Для цього необхідно провести роз'яснювальні бесіди, поширити короткі наочні навчальні матеріали та пам'ятки на тему інформаційної безпеки та соціальної інженерії.

2.7 Продукти з надання віддаленого доступу

Для організації віддаленого доступу можна скористатися програмами типу TeamViewer, Remote Desktop і Virtual Network Computing (VNC). Суть усіх цих продуктів полягає у наданні співробітнику віддаленого доступу до його робочого столу через підключення до нього клієнта (робочої станції співробітника).

2.7.1 TeamViewer

Утиліта дозволяє підключитися до комп'ютера, на якому встановлено TeamViewer. Це більше нагадує телефонний дзвінок, де як номер використовується ID користувача. За допомогою ідентифікатора користувач може знайти необхідного абонента та встановити зв'язок. Кожному присвоюється унікальний ID, який створюється виходячи з особливостей і характеристик апарата. Надалі отриманий при першому запуску номер не змінюється. [19]

Застосування TeamViewer не рекомендується через його сумнівну безпеку, оскільки він:

- використовує слабкі парольні політики. У кіберзлочинця є можливість сканування списку доступних адрес TeamVeawer, після чого підібрати, наприклад, грубим перебором, пароль до сесії і отримати доступ до робочої станції;

- надає кожному співробітнику окрему точку входу, через що стає неможливо розібратися у підключенні та гарантувати його якість.

TeamViewer можна використовувати лише під контролем у разі технічної підтримки. Використовувати TeamViewer лише під час надання послуг та закривати відразу після її закінчення.

2.7.2 Remote Desktop

Remote Desktop працює через RDP (Remote Desktop Protocol) - протокол підключення користувача до віддаленого робочого столу через сервер терміналів. Технологія з'явилася у 90-х роках і досі використовується. Розробка повністю пропрієтарна, постачається лише в операційних системах сімейства Windows.

Принцип роботи RDP базується на протоколі TCP. Поєднання клієнт-сервер відбувається на транспортному рівні. Після ініціалізації користувач проходить автентифікацію. У разі успішного підтвердження, сервер передає клієнту управління.

Протокол RDP підтримує віртуальні канали, через які користувачеві передаються додаткові функції операційної системи, наприклад, можна роздрукувати документ, запустити відео або скопіювати файл у буфер обміну. [18]

2.7.3 TightVNC

Virtual Network Computing — протокол надання доступу до віддаленого комп'ютера у мережі TCP/IP з будь-якого іншого комп'ютера чи мобільного пристрою з метою моніторингу та дистанційного керування. Для здійснення такої взаємодії потрібно встановити програмне забезпечення VNC, яке показує у вікні вашого комп'ютера весь екран (десктоп) віддаленого комп'ютера та передає йому коди натиснутих клавіш та команди комп’ютерної миші, таким чином надаючи користувачеві повний «ефект присутності».

VNC складається з двох частин: клієнта та сервера. Сервер — це програма, яка надає доступ до екрана комп'ютера, на якому вона запущена. Клієнт (або viewer) - програма, яка отримує зображення екрана із сервера.

TightVNC підтримує практично всі загальновідомі операційні системи: Windows, Linux, macOS.

VNC-клієнт, званий VNC viewer, запущений на одній операційній системі, може підключатися до VNC-сервера, що працює на будь-якій іншій ОС. Існують реалізації клієнтської та серверної частини практично для всіх операційних систем, у тому числі і для Java (включно з мобільною платформою J2ME). До одного VNC-серверу одночасно можуть підключатися численні клієнти.

Порівняння деяких можливостей додатків з надання віддаленого доступу наведено у таблиці 2.3.

Таблиця 2.3 – Порівняння додатків з надання віддаленого доступу

Можливості	TeamViewer	Remote Desktop	VNC
Ручне встановлення пароля	-	+	+
Ручне встановлення адреси сесії	-	+	+
Вибір порту для підключення	-	-	+
Кросплатформеність	+	-	+
Можливість конфігурації клієнта та сервера	-	+	+

2.8 Хмарні послуги з віртуалізації робочих столів

Під час термінового переходу на дистанційний формат роботи бізнес зіткнувся з новими навантаженнями на IT-інфраструктуру. Навіть технологічно розвинені компанії змушені були перерозподіляти потужності, щоб забезпечити працездатність корпоративних ресурсів при віддалених підключеннях.

Щоб організувати безпечну дистанційну роботу, потрібно підготуватися до цього заздалегідь. Якщо раніше в організації працювало більше 15 співробітників без централізованої системи безпеки, перейти на віддалену роботу буде досить складно. Коли адміністратори закуповують та налаштовують обладнання поспіхом, помилок не уникнути. Виходом може бути оренда хмар. Це недешевий сервіс, але дозволяє швидко отримати безпечні ресурси.

VDI (Virtual Desktop Infrastructure) - це концепція, у якій дані з ПК співробітника зберігаються централізовано, а кожний співробітник має віртуальний ПК. Це зручно бізнесу, тому що на жорсткому диску співробітника вже немає жодних бізнес-даних. Адміністратор сервера створює віртуальне робоче місце з окремим набором додатків, програм, документів та доступів, які зберігаються на сервері – у ЦОД. Підключення та вся робота співробітника йде через «прошарку» — «тонкий клієнт» [11]. Приклад того, як влаштована схема VDI зображено на рисунку 2.5.

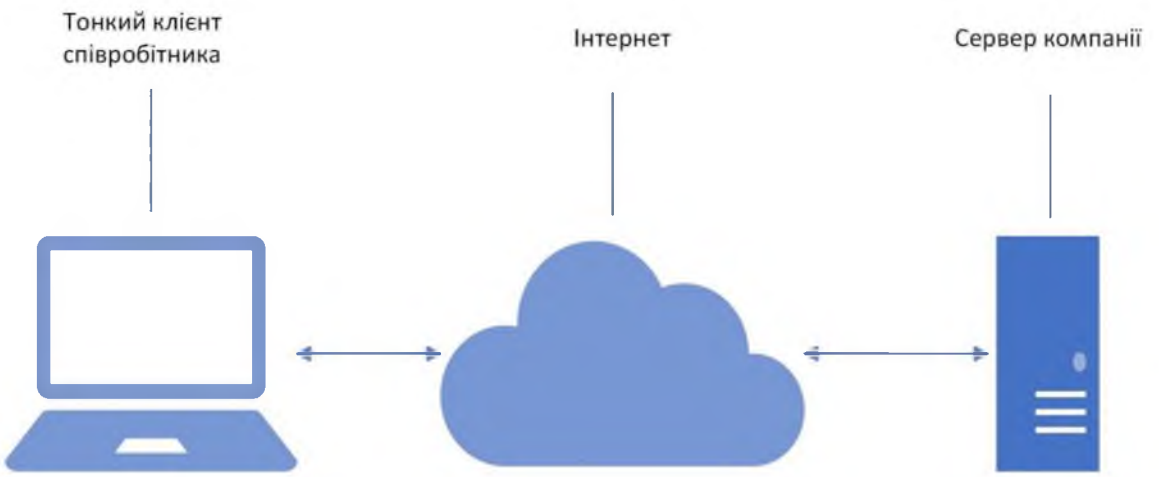


Рисунок 2.5 – Приклад схеми VDI

Віртуалізація робочих столів допоможе крупним мережевим компаніям:

- для масштабування - організації нових філій;
- для окремих підрозділів, наприклад, у call-центрах;
- для віддалених офісів – жорсткого обмеження прав користувачів;
- для зниження капітальних витрат на IT-інфраструктуру.

Для співробітника з VDI нічого не змінюється - на екрані той самий робочий стіл, та ж ОС та програми. Але така система зручніша для IT-департаменту завдяки кільком перевагам:

- безпека;
- централізоване керування;
- економія.

2.8.1 Безпека

Витоки даних трапляються як у маленьких кав'ярень, так і у корпорацій. Саме тому на чорному ринку з'являються дані кредитних карток великих банків або записи call-центрів операторів зв'язку.

Зазвичай слабка ланка в безпеці — це людина. Співробітник може взяти роботу додому, стати жертвою корпоративного шпигунства або випадково завантажити шкідливий файл. Крім того, жорсткий диск виходить з ладу через природний знос, сильну вібрацію або випадковий удар, а частину даних можуть випадково видалити.

Як VDI вирішує ці проблеми:

- усі дані, конфіденційна інформація та комерційна таємниця зберігаються не на жорсткому диску комп'ютера співробітника, а в дата-центрі;

- дата-центр захищений краще ніж персональний ПК: резервуванням, резервним харчуванням, фізичною охороною, пожежними системами. Вимкнення світла в офісі не призведе до втрат – віртуальний робочий стіл буде також доступний із будь-якої точки світу з інтернетом. Це підвищує доступність та катастрофостійкість.

- системний адміністратор клієнта завжди бачить, що відбувається у віртуальних ПК. Налаштовані скрипти за підозрілої активності блокують робоче місце. За наявності списку доступних користувачеві програм, які дозволив системний адміністратор, користувач не зможе завантажити шкідливі програми.

2.8.2 Централізоване управління

VDI полегшує керування робочими місцями. Зазвичай системні адміністратори та керівники IT-підрозділів працюють із купою додатків, ліцензій та офісної техніки різних постачальників з різним терміном використання. Обслуговування займає багато часу, а хаос ускладнює використання єдиних рішень та стандартів.

З віртуалізацією централізоване управління набагато простіше, завдяки наступним можливостям:

- налаштовувати резервне копіювання, оновлювати програмне забезпечення, керувати трафіком, стежити за діями користувачів набагато зручніше з однієї точки;

- коли потрібне нове робоче місце, адміністратор створює його за пару хвилин (або автоматично) та видаляє також швидко;

- для розгортання та оновлення програм на віртуальних машинах оновити потрібно лише образ, а не кожен фізичний ПК;

- вік ПК не впливає на роботу: всі користувачі на різному устаткуванні отримають єдину продуктивність.

Перевага централізації особливо помітна для компаній із філіалами або віддаленими офісами. З VDI адміністратор управляє десятками комп'ютерів у різних філіалах у різних містах з одного кабінету із центрального офісу. Це економія часу, витрат на відрядження та штат технічної підтримки.

2.8.3 Економія

Це наслідок попередніх пунктів – централізоване управління зменшує витрати. Наприклад, закупити робочу станцію ПК для десятків співробітників, встановити ОС, налаштувати тощо – це великі витрати грошей та часу. Для VDI потрібно набагато менше інфраструктури: знадобиться сервер, монітор і тонкий клієнт. При цьому тонкий клієнт простіше і швидше налаштувати.

VDI має низькі вимоги до клієнтської частини, тому тут можна заощадити, як на оновленні заліза, так і на «тонких клієнтах». Представимо невелику підрядну організацію: більше 15 робочих місць та застарілий парк ПК. Оновити все одразу дорого, а оновлювати частинами і розтягнути на місяці — некомфортно для співробітників. VDI – це компромісний варіант: витягти з комп'ютерів все зайве, зарезервувати сервер, оплатити ліцензії, налаштувати високошвидкісний інтернет та перейти на VDI.

Економія в тому, що будь-який ПК можна перетворити на тонкий клієнт. Це одразу зменшує витрати на операційне обслуговування: не потрібно оновлювати парк техніки, із графи «витратні матеріали» зникають жорсткі диски та інші комплектуючі. Менше «начинки» у фізичних машин менше обслуговування.

Менше обслуговування — менший за штат технічної підтримки. Зменшується кількість інцидентів, які потрібно вирішувати на робочому місці працівника. ПК однакові, тому більшість робіт стандартизовані. Наприклад, відновлення віртуальної машини справа кількох хвилин, як і заміна тонкого клієнта. Тонкий клієнт може безперебійно працювати той самий термін, як і ПК, споживаючи менше енергії. Замінивши навіть десяток ПК на віртуальні, буде помітна різниця у платіжках за електрику.

2.8.4 VMmanager

Одним з найкращих рішень VDI є VMmanager. У VMmanager для організації віддаленого робочого столу за технологією VDI достатньо створити віртуальну машину та встановити додаткове програмне забезпечення за допомогою скриптів. Віртуальні машини можна створювати за шаблоном або налаштувати потреби конкретного співробітника.

Щоб підключитись до робочого столу, співробітник може використовувати будь-який VNC-клієнт.

VMmanager робить технології віртуалізації доступними будь-яким компаніям. З його допомогою можна створювати віртуальні машини на Linux і Windows як для продажу, так і для власних потреб.

Хостинг-провайдери використовують VMmanager для надання послуг віртуальних машин. Веб-розробники, центри навчання, комерційні організації та інші користувачі з допомогою створюють ізольовані віртуальні машини.

Панель має простий і зручний інтерфейс. З ним більшість процесів можна автоматизувати, а виконання інших сильно прискорити.

Інші переваги VMmanager:

- все в одному місці: панель замінює консоль, таблиці для обліку обладнання, інструменти діагностики та моніторингу.

- простий та зручний інтерфейс: кінцевий користувач легко зможе сам створити ВМ потрібної конфігурації, адміністратор заощадить час на налаштуванні.

- управління завданнями: якщо виникне проблема, через журнал завдань на панелі легко знайти причину. [4]

2.9 Захист від інсайдерських загроз

У період масового переведення компаній на режими віддаленої роботи збільшився попит на спеціалізовані рішення для моніторингу активності співробітників.

Причина проста: роботодавці хочуть знати, чим співробітники зайняті поза їхнім полем зору, щоб переконатися, чи вони дійсно працюють, а не безцільно «сидять» в інтернеті.

В офісі не доводиться спеціально контролювати робочий час, тому що діє корпоративна культура: співробітники починають робочий день о 8-й, йдуть на обід і повертаються з нього.

У віддаленому режимі роботи стежити за робочим графіком складніше. Відповідальні співробітники, які мають багато роботи, можуть просидіти за комп'ютером цілий день. Але таких людей не так багато. Всі інші можуть займатися своїми справами, доки ними не стежать. В усіх будинках є багато цікавих речей, які відволікають.

Виникає питання, як контролювати людей, адже не можна поставити кожному співробітнику камеру і постійно стежити за ним.

Програми для обліку робочого часу, такі як CrocoTime або Стахановець, фіксують чим співробітник займався цілий день. Ці звіти потрібні не тільки для того, щоб їх дивилися, вони використовуються як «театр безпеки». Коли

людина знає, що за її діями стежать, вона дотримуватиметься робочого часу і намагається працювати продуктивно. Це корисна річ, яку можна використати.

2.10 Крадіжка даних співробітниками

Існують випадки, коли після переходу на віддалення у компанії в кілька разів падали продажі. При цьому кількість клієнтів не змінилася: клієнти, як і раніше, зверталися до менеджерів, але угоди не укладалися.

Коли співробітники працюють в офісі, вони негласно наглядають один за одним. Ніхто не буде: фотографуватиме екран, пересилати інформацію з обмеженим доступом електронною поштою або переказуватиме її телефоном.

Цінність інформації, яку можна вкрасти, сфотографувавши екран, є великою. Особливо це стосується компаній які працюють з великим капіталом: зі сфери нерухомості або автомобільного бізнесу. У цих компаніях дуже цінний навіть номер телефону клієнта.

Менеджери, які його бачать, можуть обробити заявку у своїй компанії та не отримати нічого, крім зарплати. А можуть продати інформацію конкурентам та отримати бонуси. Компанія втратить клієнта, зазнає фінансових та репутаційних втрат.

Єдиний захист від крадіжки таких клієнтів – захистити його контактні дані від людини, яка з ними працює. Для цього в CRM-системі має бути прихований номер телефону. Така можливість є, наприклад, у 1С-Рарус: Call Center. У ній номери не відображаються.

Телефонна станція сама робить дзвінок. Оператору надходить вже знеособлена інформація: «Телефонує клієнт Володимир». CRM не має жодної інформації, яку можна з вигодою вкрасти. Такі програми не вбережуть від топових співробітників, які зазвичай мають доступ до всієї інформації та від технічних співробітників, які обслуговують систему. Але ризик втратити клієнта зменшиться. [3]

2.11 Чек-лист співробітника кібербезпеки

Щоб врахувати основні фактори, що впливають на захищеність організації при переведенні працівників на віддалений режим роботи, компанією Positive Technologies було складено невеликий чек-лист, який можна використовувати для самоперевірки [1]. Його наведено у таблиці 2.4.

Чого побоюватися	Що робити
Підбір паролів та проникнення зловмисника в мережу організації:	- перевірити та посилити парольні політики.
Розкрадання конфіденційної інформації:	- розмежувати права доступу до внутрішніх ресурсів; - посилити контроль доступу до інформації та її передачі.
Зараження пристроїв співробітників та розповсюдження ВПЗ на ресурси компанії:	- захистити особисті гаджети; - перевірити поштові вкладення; - підвищити ІБ-обізнаність працівників.
Атака через незахищені сервіси віддаленого доступу, що з'явилися на периметрі:	- моніторити мережевий периметр; - виключити пряме підключення до окремого робочого місця, використовувати шлюзи для віддаленого підключення.
Неможливість виявити та зреагувати на нелегітимні дії співробітників та атаки:	- журналувати події ІБ, у тому числі на віддалених пристроях співробітників; - зберігати копії мережевого трафіку; - моніторити ІБ-події; - аналізувати мережевий трафік.
Несвоєчасне реагування на інциденти, неможливість оперативно зупинити атаку:	- організувати SOC (security operation center) 24x7; - моніторити системи захисту 24x7.
Компрометація ключових бізнес-систем організації внаслідок атаки:	- сегментувати внутрішні мережі; - контролювати доступ до ключових сегментів та систем.
Порушення безперервності бізнес-процесів через збої при віддаленому підключенні працівників до внутрішніх ресурсів:	- резервувати канали зв'язку для віддаленого доступу; - використовувати кілька незалежних способів віддаленого доступу (наприклад: VPN та RDP); - резервувати сервери віддаленого доступу та розподіляти навантаження між ними.
Відмова бізнес-систем через підвищене навантаження або внаслідок атаки на відмову в обслуговуванні:	- технічна підтримка з боку IT-підрозділів компанії 24x7.

2.12 Встановлення та конфігурація архітектурного рішення

Проаналізувавши пункти вище, я вибрав наступний програмно-апаратний комплекс для забезпечення безпеки віддаленого робочого місця співробітника компанії:

- робоча станція – тонкий клієнт;
- програмне забезпечення для сервера Windows Server
- VNC клієнт – TightVNC;
- VDI сервіс - VMmanager KVM.

Адміністратор конфігурує сервер за допомогою VMmanager'а, виділяючи потрібну кількість віртуальних робочих столів для співробітників компанії.

Кожному працюючому вдома співробітнику розсилається налаштований тонкий клієнт від підприємства. Співробітники встановлюють його, підключають до нього мережевий кабель та запускають. Після цього співробітник підключається до своєї віртуальної робочої станції, що знаходиться на сервері компанії, через VNC-клієнт, що встановлено на їх тонкому клієнті, та отримує інтерфейс своєї робочої станції, завдяки сконфігурованому управлінню віртуальними машинами VMmanager'а. Під час роботи співробітник натискає клавіши та маніпулює мишкою, ці натискання та маніпуляції, передаються на сервер, а він, в свою чергу, передає їх на віртуальну робочу станцію співробітника. По завершенню цього, віртуальна машина передає серверу результат операцій співробітника, тобто свій інтерфейс, а сервер передає його VNC-клієнту співробітника.

У зв'язку з цим, на підприємстві з'явиться два нових інформаційних потоки, які наведені у таблиці 2.5.

Таблиця 2.6 – Інформаційні потоки VNC

№	Дані, які обробляються
9.	Натиснуті клавіши та рухи миші
10.	Інтерфейс віртуальної машини

Приклад того, як буде організовано віддалений доступ для співробітника, зображено на рисунку 2.6.

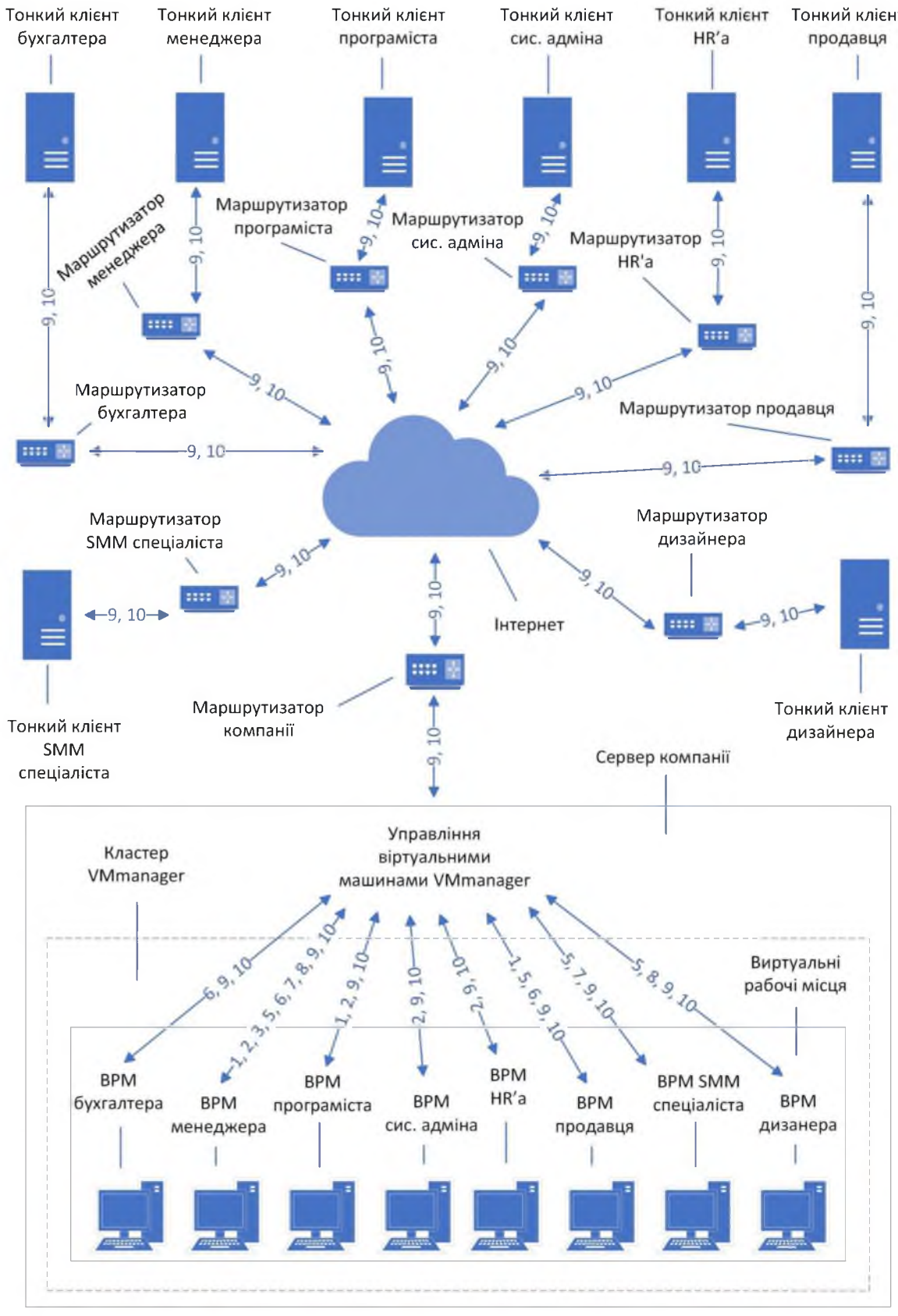


Рисунок 2.6 – Інформаційні потоки організації у режимі віддаленого доступу для співробітника

Співробітник компанії працює віддалено. Для нього створено віртуальний робочий стіл. Якщо потрібно підготувати інший віддалений робочий стіл, адміністратор може швидко створити його, застосувавши готовий шаблон. Кластер з усіма віртуальними серверами знаходиться в офісі компанії, що дозволяє системному адміністратору керувати всім обладнанням з однієї точки. У кластері створено віртуальний робочий стіл для співробітника. [5]

2.12.1 Створення завантажувальної флешки з дистрибутивом Windows Server

1. Необхідно мати флешку щонайменше 8 гб пам'яті;

2. Далі завантажуємо програму для запису дистрибутива Windows Server [22] на флешку за цим посиланням - [23];

3. Відкриваємо програму WinSetupFromUSB-1-6 та робимо такі дії:

- вибрати флешку;
- натиснути на галочку з Auro Format;
- вибрати тип файлової системи NTFS;
- вказати нехай до дистрибутива Windows Server;
- натиснути кнопку "GO".

Приклад вікна зображено на рисунку 2.7.

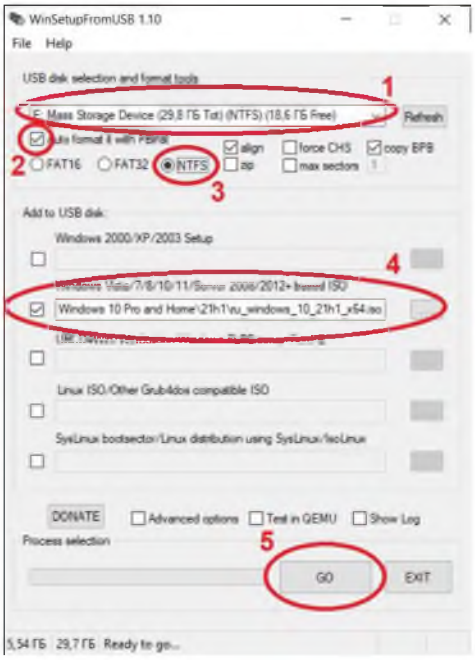


Рисунок 2.7 – Головне вікно програми WinSetupFromUSB 1.10

4. Потім з'являться два вікна поспіль, у яких потрібно натиснути кнопку "Так", після чого дочекатися завершення запису дистрибутива на флешку. Приклади вікон зображено на рисунках 2.8 та 2.9.

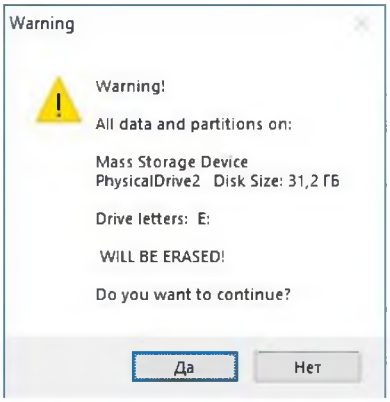


Рисунок 2.8 – Перше попередження про знищення даних

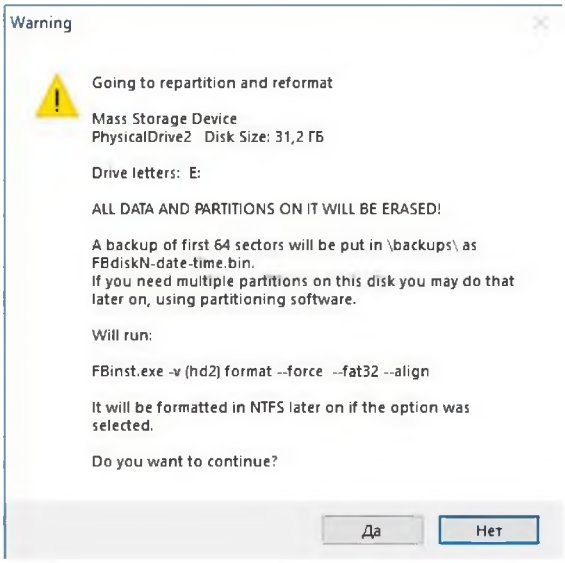


Рисунок 2.9 – Друге попередження про знищення даних

2.12.2 Завантаження з флешки з-під BIOS

1. Щоб зайти в BIOS, необхідно відразу при включенні сервера затиснути кнопку «Delete» на клавіатурі. [24]

2. Після того, як BIOS завантажиться, потрібно визначити Boot меню і змінити пріоритет завантаження, на флешку, перемістивши її на перше місце в черзі накопичувачів. Приклад вікна зображено на рисунку 2.10.

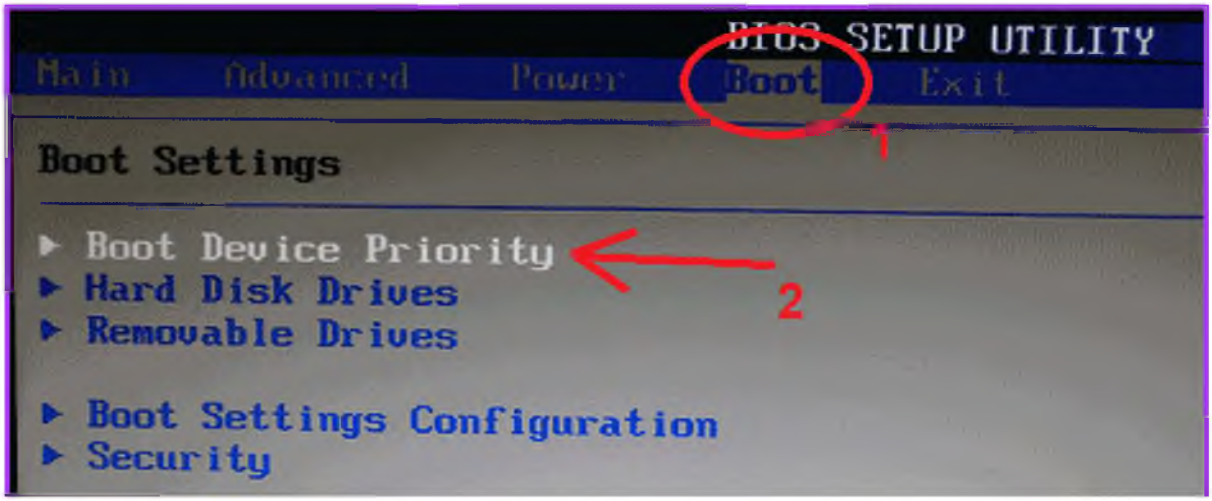


Рисунок 2.10 – Boot меню BIOS'а

3. Далі необхідно натиснути клавішу F10 та прийняти умови перезавантаження.

2.12.3 Встановлення Windows Server на сервер та його первинне налаштування

1. Після завантаження з флешки розпочнеться інсталяція Windows Server. У вікні, необхідно вибрати потрібну мову в кожному з трьох пунктів, натиснути «Далі», а потім, «Встановити». Вікна зображено на рисунках 2.11 та 2.12.

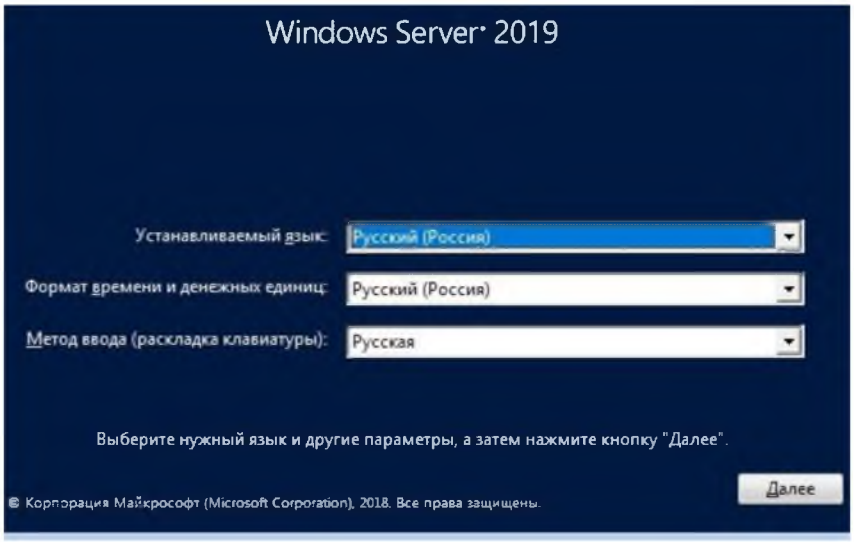


Рисунок 2.11 – Вікно вибору мови системи

Рисунок 2.12 – Запрошення інсталювати систему

2. Тепер потрібно вибрати стандартну редакцію Windows Server із можливостями робочого столу та натиснути кнопку «Далі». Приклад вікна зображено на рисунку 2.13.

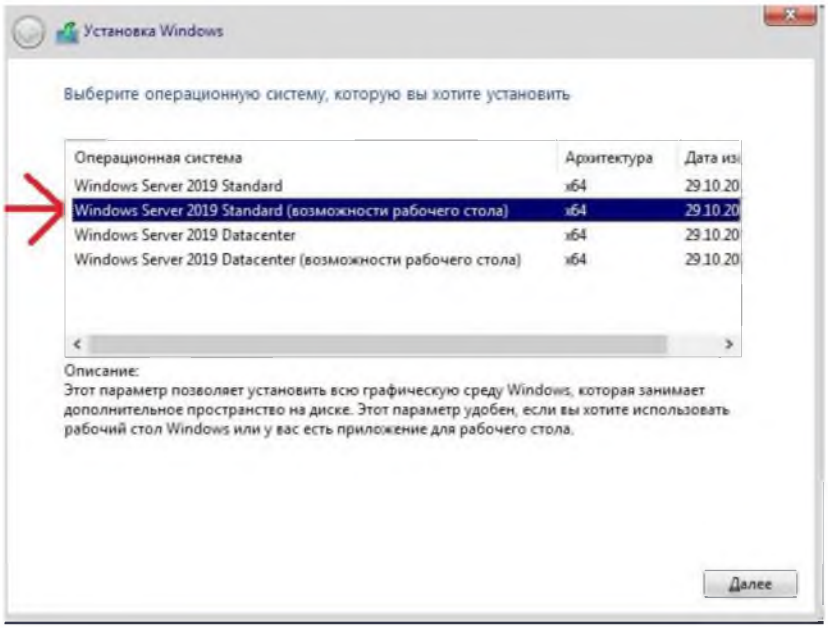


Рисунок 2.13 – Вибір операційної системи

3. Зараз необхідно прийняти умови ліцензування та натиснути кнопку «Далі». Приклад вікна зображено на рисунку 2.14.

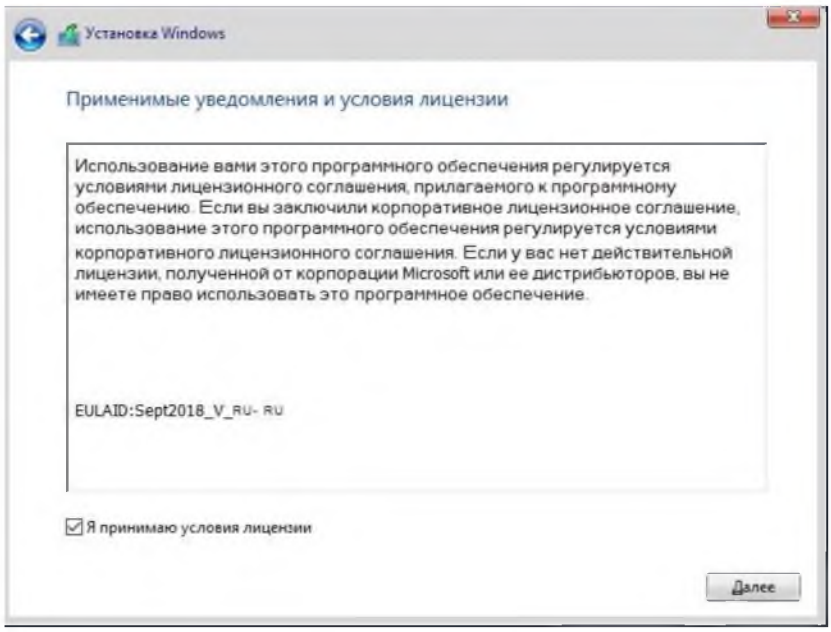


Рисунок 2.14 – Ліцензійні умови

4. Потім необхідно обрати вибіркову установку. Приклад вікна зображено на рисунку 2.15.

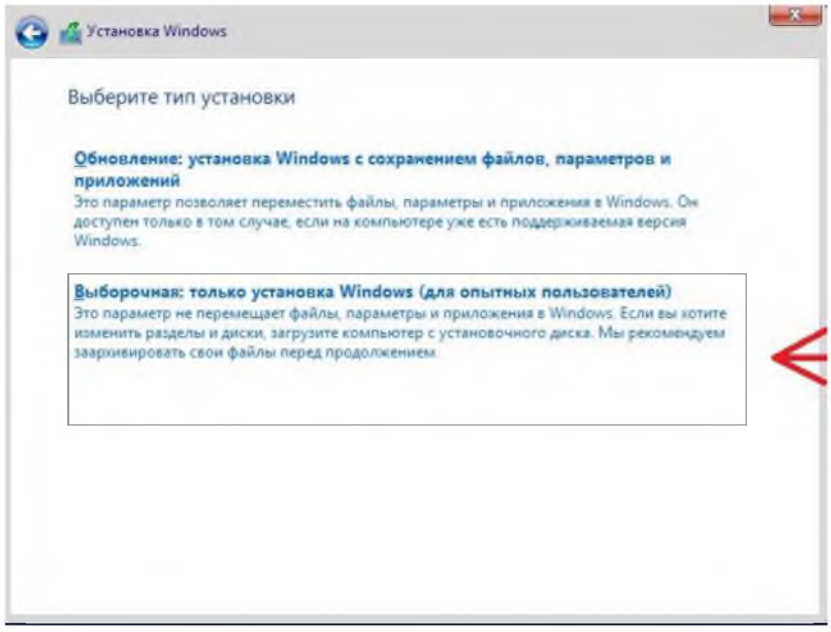


Рисунок 2.15 – Тип встановлення

5. Тепер потрібно вибрати диск, на який буде встановлена система та натиснути кнопку «Далі». Приклад вікна зображено на рисунку 2.16.

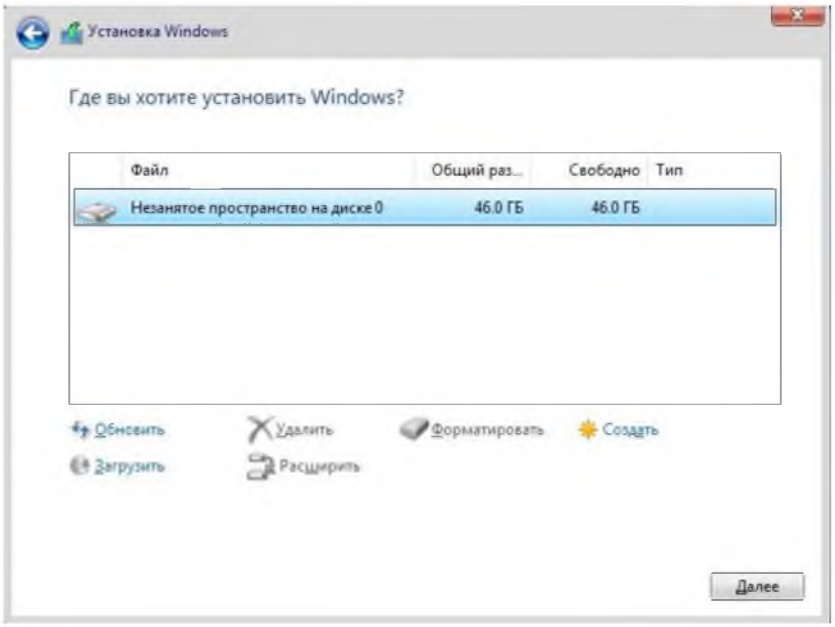
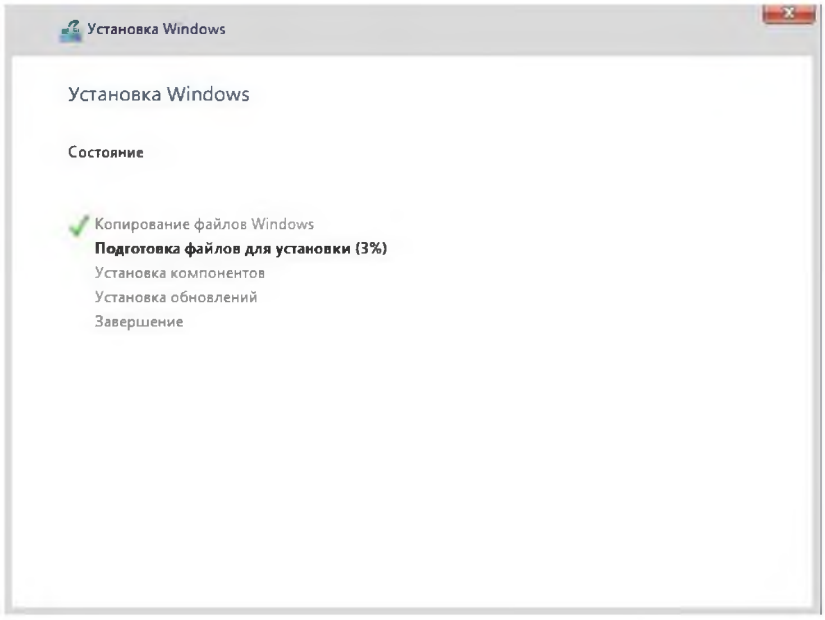


Рисунок 2.16 – Вибір диску

6. На цьому етапі слід дочекатися закінчення установки, під час якої система перезавантажиться кілька разів. Приклади вікон зображено на рисунках 2.17 та 2.18.



2.17 – Статус встановлення системи

2.18 – Вікно після перезавантаження

7. Після того, як система буде встановлена, знадобиться задати пароль задати пароль для облікового запису адміністратора та натиснути кнопку «Готово». Приклади вікон зображено на рисунках 2.19 та 2.20.

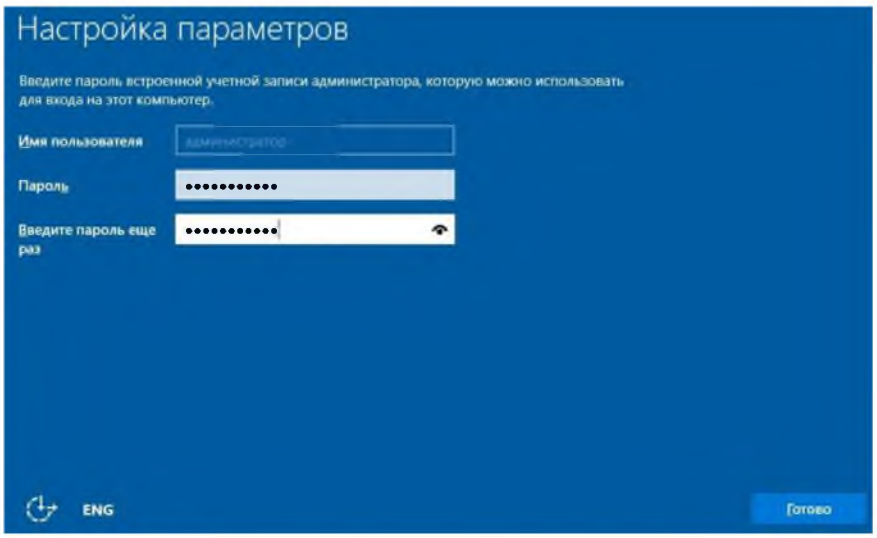


Рисунок 2.19 – Налаштування параметрів

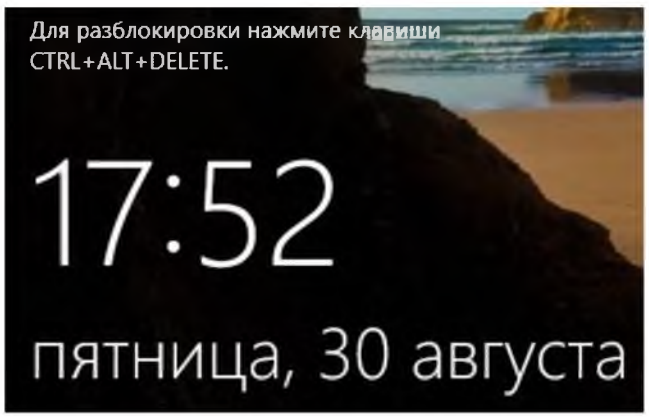


Рисунок 2.20 – Вікно очікування входу до облікового запису користувача

8. Тепер потрібно авторизуватися під обліковим записом адміністратора для входу до системи. Приклад вікна зображено на рисунку 2.21.

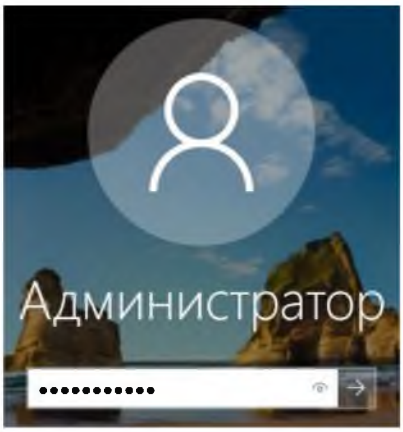


Рисунок 2.21 – Вікно авторизації

9. Тепер, відразу після установки системи, потрібно її активувати та завантажити всі актуальні оновлення. Необхідно зайти в меню «Властивості системи», потім натиснути «Активація Windows», далі «Змінити ключ продукту», ввести ключ активації системи в полі введення натиснути «Далі», потім «Активувати» та в наступному вікні «Закрити». Приклади вікон зображено на рисунках 2.22, 2.23, 2.24 та 2.25.

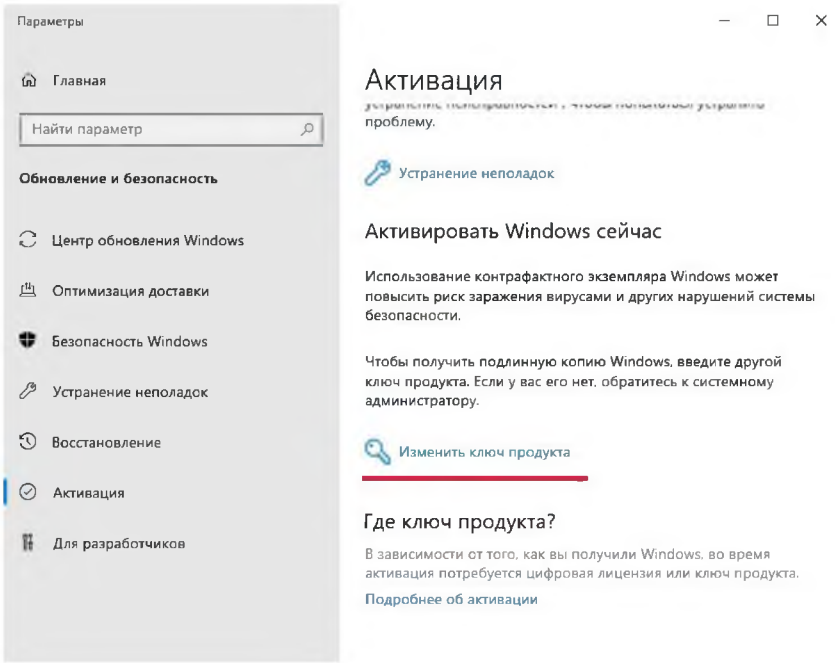


Рисунок 2.22 – Активація системи

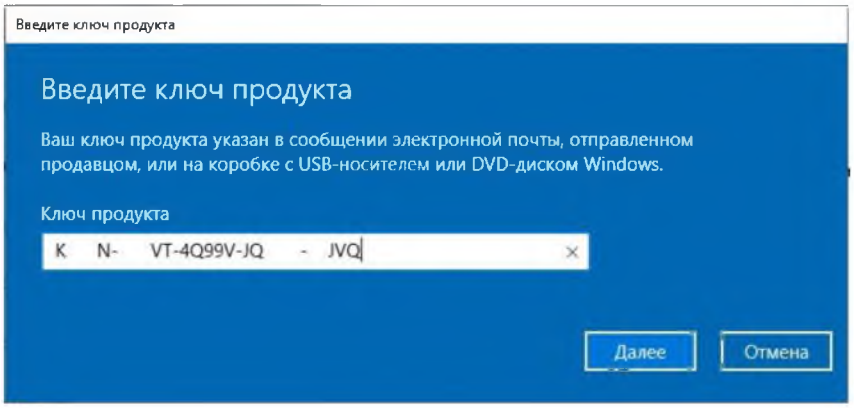


Рисунок 2.23 – Запрошення ввести ключ продукту

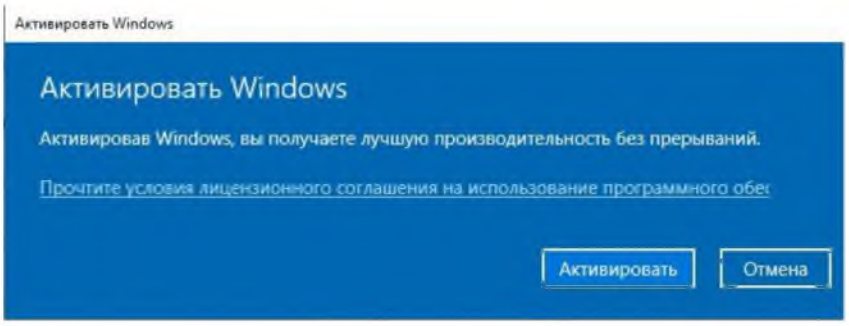


Рисунок 2.24 – Запрошення активувати систему

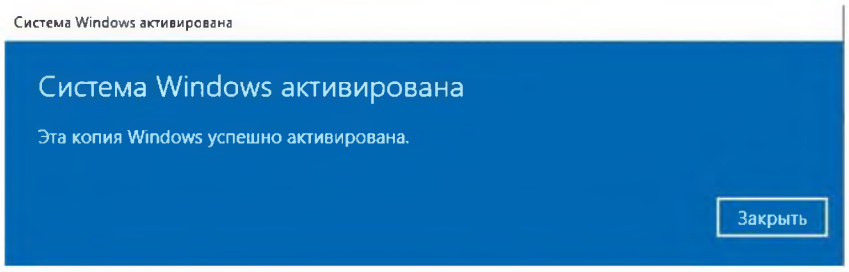


Рисунок 2.25 – Повідомлення про успішну активацію

10. Після активації необхідно переконатися, що система була активована. Потрібно знову перейти в меню «Властивості системи» та перевірити активацію. Приклад вікна зображено на рисунку 2.26.

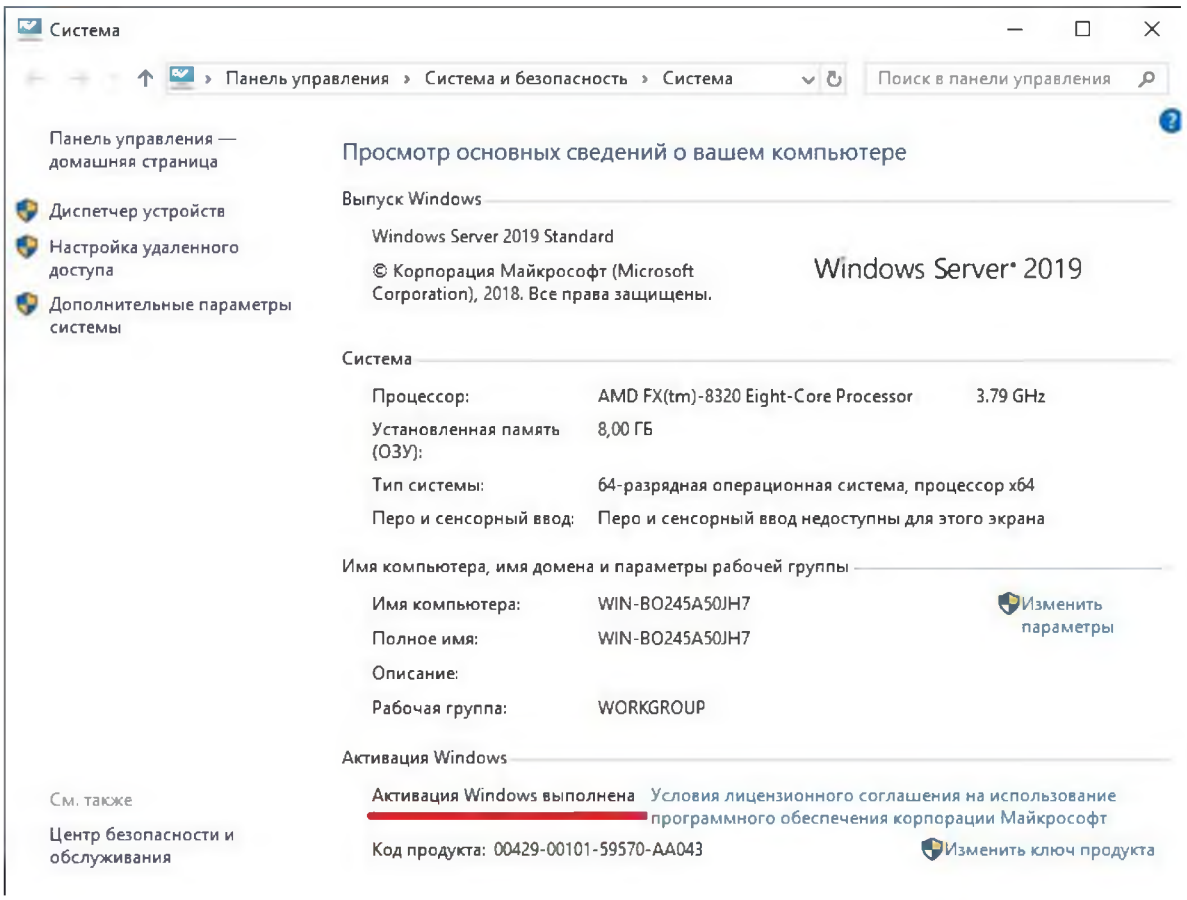


Рисунок 2.26 - Відомості про комп'ютер

11. Тепер необхідно завантажити та встановити актуальні оновлення системи. Треба натиснути кнопку з іконкою збільшувального скла (лупи) праворуч від кнопки «Пуск» і ввести слово оновлення, після чого вибираємо запропонований варіант меню в списку пошуку «Перевірити наявність оновлень», а в наступному вікні, натискаємо однойменну кнопку «Перевірити наявність оновлень». Якщо оновлення доступні для завантаження та встановлення, натискаємо кнопку «Завантажити та встановити зараз», після чого потрібно буде перезавантажити систему. Приклади вікон зображено на рисунках 2.27, 2.28 та 2.29. [21]

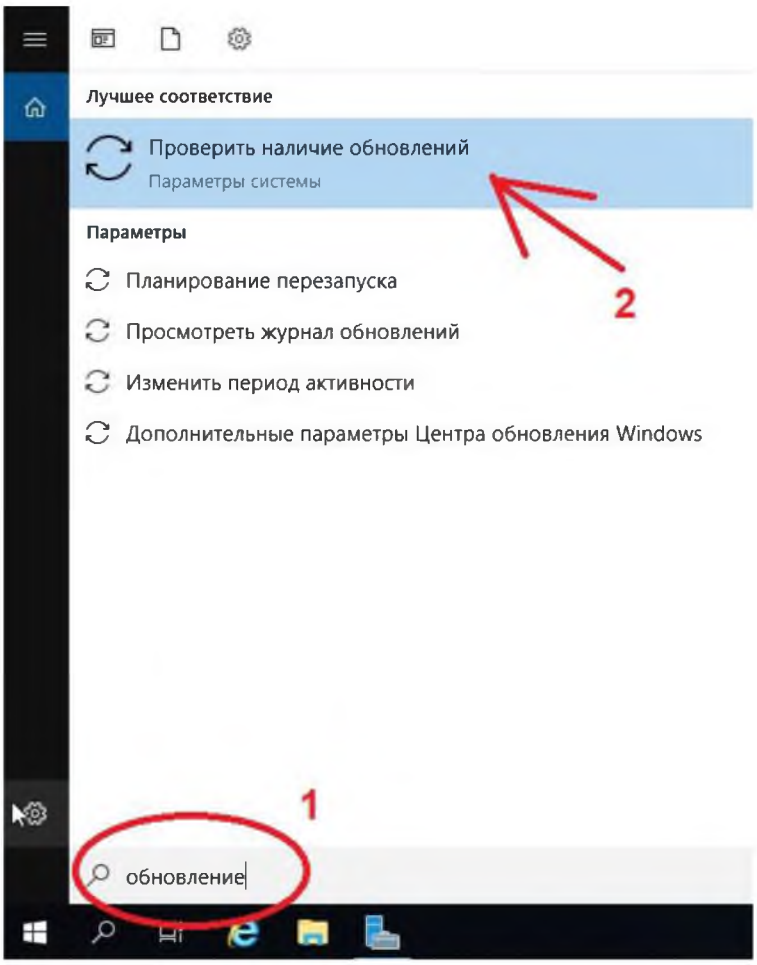


Рисунок 2.27 – Вікно пошуку

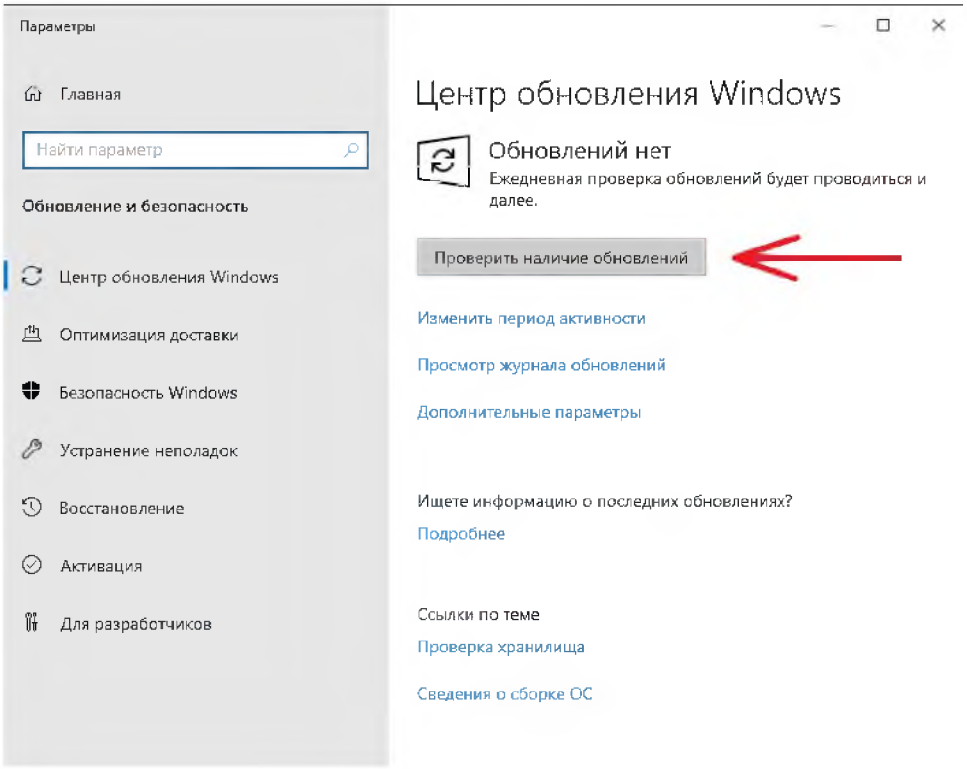


Рисунок 2.28 - Центр оновлень з запрошенням їх перевірити

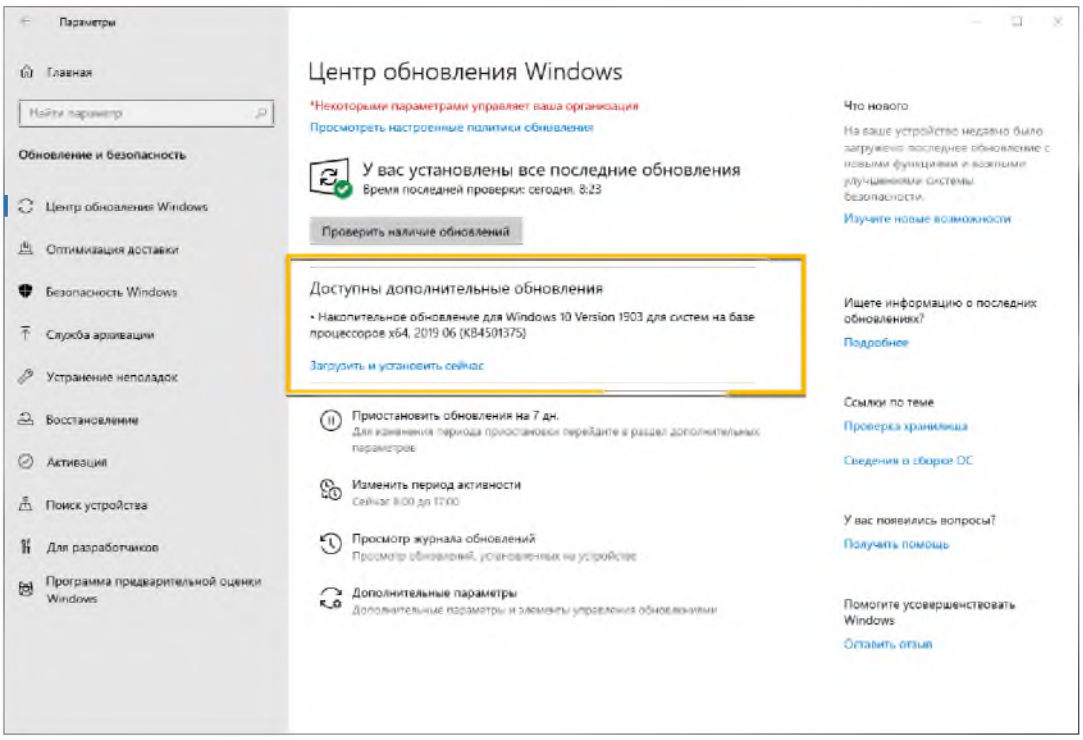


Рисунок 2.29 - Центр оновлень з запрошенням їх завантажити та встановити [25]

2.12.4 Встановлення та конфігурація VMmanager'a

1. У терміналі необхідно встановити утиліту для завантаження файлів ввівши команду [26]:

yum install wget

2. Потім потрібно завантажити встановлювача продуктів ispsystem командою:

wget http://cdn.ispsystem.com/install.sh

3. Для початку встановлення необхідно ввести команду:

sh install.sh --release 5.221.0 VMmanager

4. Тепер потрібно обрати, яка версія VMmanager буде встановлена (KVM або OVZ), відповівши на запитання введенням 1, після чого буде виконано завантаження та встановлення необхідних пакетів із конфігурацією сервера для коректної роботи. Після завершення встановлення потрібно зайти в браузер і перейти за адресою "https://<IP-адреса::1500/vmmgr", де, можливо, буде показана помилка сертифіката, яку потрібно проігнорувати і продовжити завантаження. Потім з'явиться вікно з пропозицією активувати продукт, де потрібно буде ввести ключ активації VMmanager. Приклад вікна зображено на рисунку 2.30.

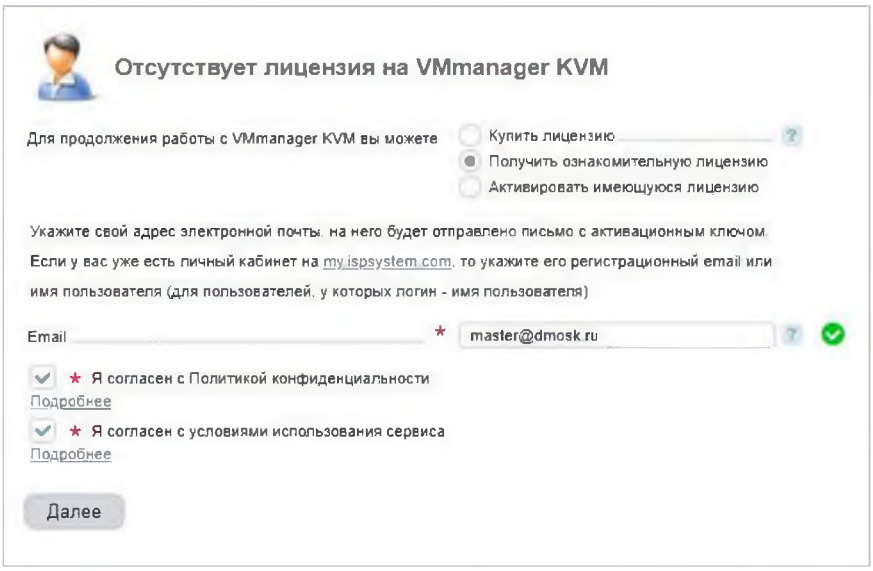


Рисунок 2.30 – Статус ліцензії VMmanager

5. На цьому встановлення завершено. Тепер потрібно зайти в панель, а потім у VMmanager для його конфігурації. Спочатку налаштування політики. Для цього потрібно перейти в розділ «Налаштування кластера», потім «Політики» та налаштовати їх основні параметри. Приклади вікон зображено на рисунках 2.31 та 2.32.

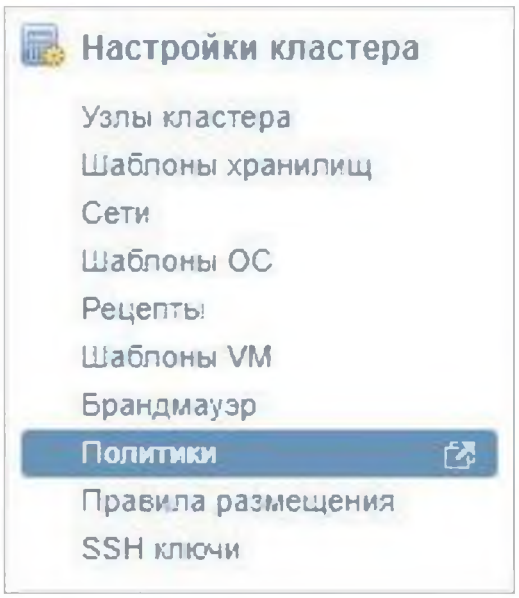


Рисунок 2.31 – Розділ налаштування кластеру

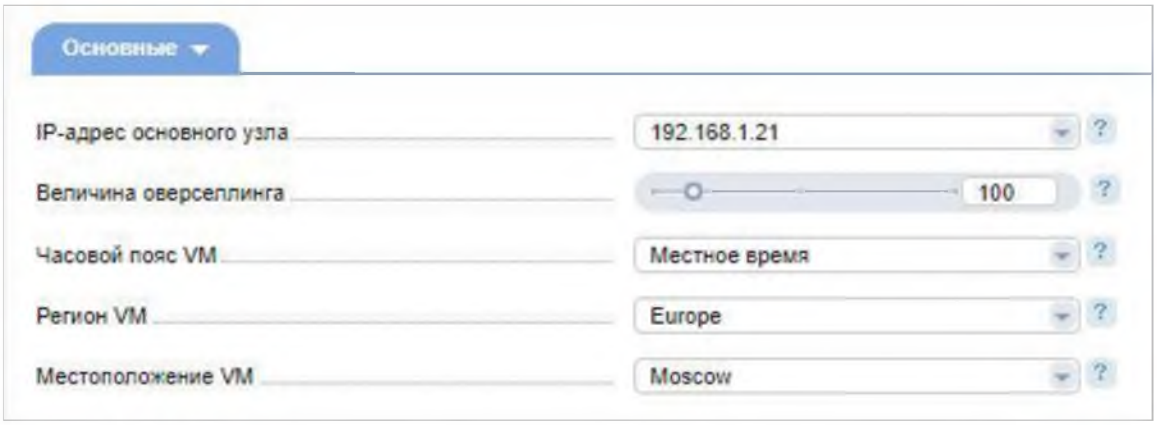


Рисунок 2.32 – Основні налаштування політик,

де IP-адреса основного вузла - адреса з мережі, в якій будуть працювати всі вузли кластера (якщо вона буде);

величина оверселлінгу — відсоток вільної пам'яті на сервері, який буде доступний виділення віртуальним машинам. Якщо на сервері можуть бути запущені інші служби, крім хоста віртуальних машин, варто скоротити цей відсоток, наприклад, до 80%;

часовий пояс VM — з яким часовим поясом створюватимуться нові віртуальні машини;

регіон VM – регіон часового поясу;

розташування VM - географічне розташування віртуальних машин.

6. Тепер необхідно виконати налаштування мережі. Приклад вікна зображено на рисунку 2.33.

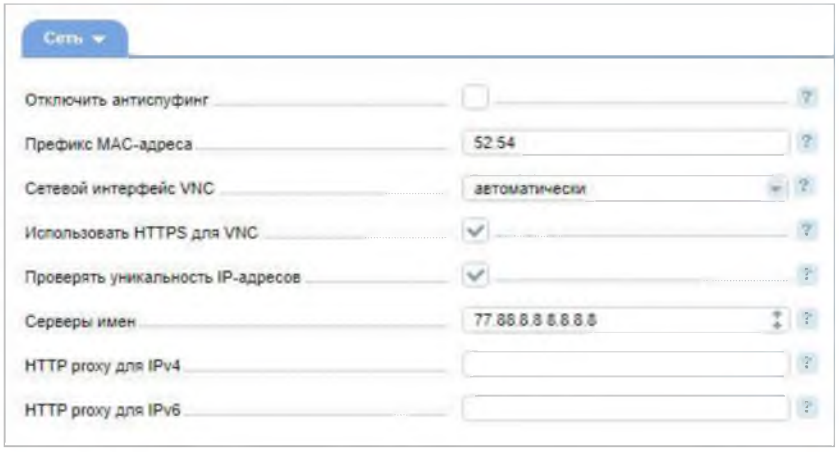


Рисунок 2.33 – Налаштування мережі,

де вимкнути антиспуфінг — відключає можливість створення правил антиспуфінгу (блокування повідомлень, надісланих від локального домену, але неавторизованої IP-адреси);

префікс MAC-адреси - перші 2 байти, які будуть у всіх MAC-адресах, згенерованих для віртуальних машин;

мережевий інтерфейс VNC — до якого інтерфейсу будуть підключені віртуальні машини для доступу до VNC. Якщо вказати «автоматично», то буде обрано той bridge-інтерфейс, до якого підключена віртуалка;

використання HTTPS для VNC — консоль VNC повинна працювати за захищеним протоколом HTTPS;

перевірити унікальність IP-адрес - при створенні віртуальної машини перевіряти IP адреси на унікальність;

сервери імен — сервери DNS, які будуть прописані в налаштування мережі після розгортання операційної системи;

HTTP proxy для IPv4 (IPv6) — якщо для HTTP-запитів необхідно використовувати проксі, вводимо його адресу у відповідні поля.

7. Далі встановити обмеження кількості образів ISO. Приклад вікна зображено на рисунку 2.34.

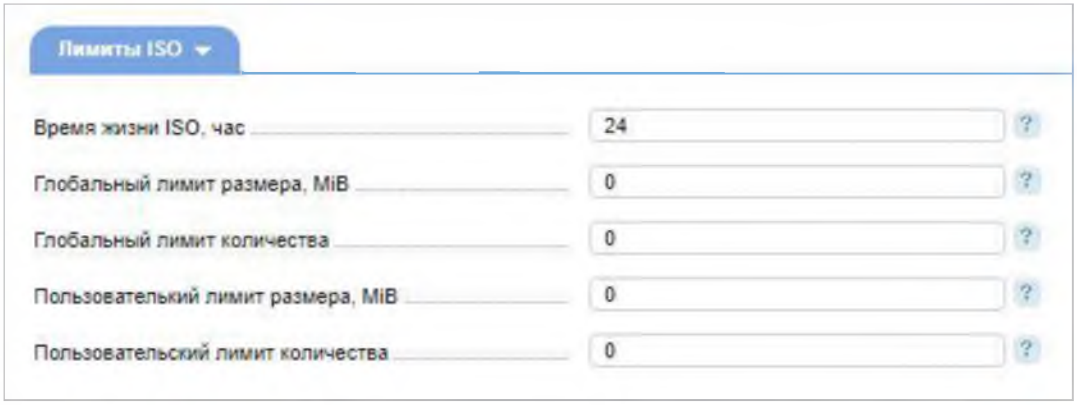


Рисунок 2.34 – Ліміти ISO,

де час життя ISO, година — через скільки годин видалити образи ISO.

глобальний ліміт розміру, MiB – максимальний розмір всіх образів ISO всіх користувачів;

глобальний ліміт кількості – максимальна кількість образів, які можуть бути створені у системі;

ліміт розміру користувача, MiB — максимальний розмір всіх образів ISO одного користувача. Вказується це значення, якщо не задається явно під час створення користувача;

ліміт кількості користувача - кількість образів, які може створити користувач.

8. Тепер необхідно налаштувати віртуальні машини, приклад з налаштуваннями яких зображено на рисунку 2.35.

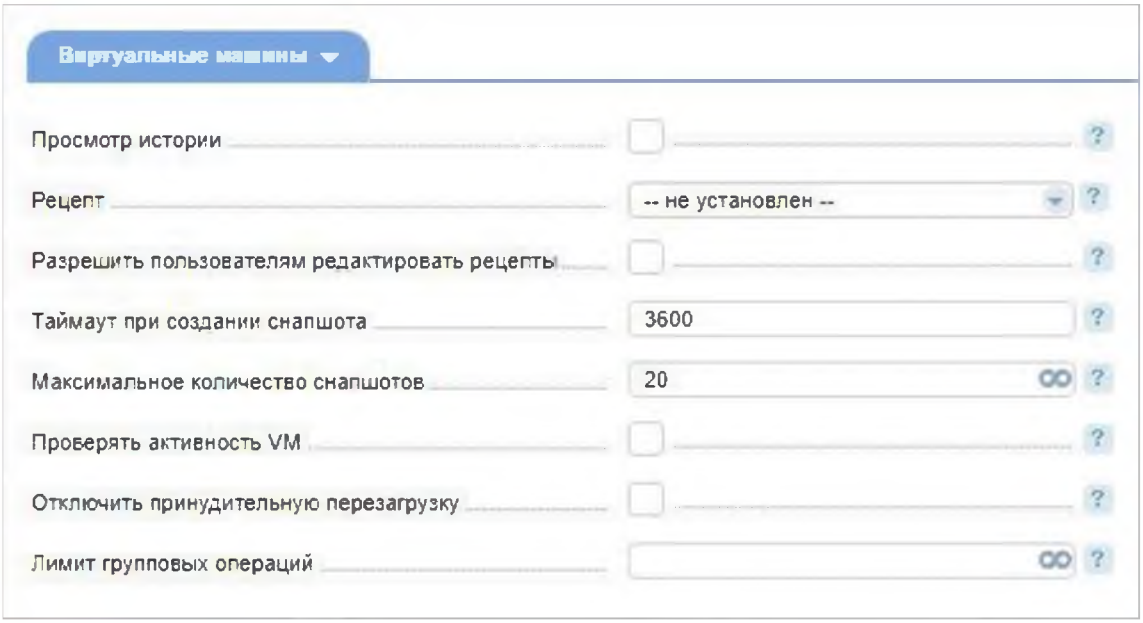


Рисунок 2.35 – Налаштування віртуальних машин,

де перегляд історії — чи дозволити користувачеві дивитися історію щодо дій над віртуальною машиною;

рецепт - після встановлення віртуальної машини її можна відразу налаштувати для виконання якогось сервісу;

дозволити користувачам редагувати рецепти — чи дозволити користувачеві самому міняти рецепти;

таймаут під час створення снапшота — час у секундах, протягом яких повинен створюватися снапшот. Інакше система поверне помилку;

максимальна кількість снапшотів – скільки можна створити снапшотів;

перевіряти активність VM - система може іноді перевіряти активність віртуальної машини та відзначати стани;

вимкнути примусове перезавантаження — вимкнути перезавантаження, яке має відбутися протягом 24 годин після зміни конфігурації віртуальної машини;

ліміт групових операцій – обмежити кількість однакових операцій над віртуальною машиною.

9. Далі необхідно налаштувати вузол кластеру. Для цього потрібно перейти в розділ «Налаштування кластера» і «Вузли кластера», після чого натиснути «Додати» і виконати налаштування у вікні. Приклади вікон зображено на рисунках 2.36 та 2.37.

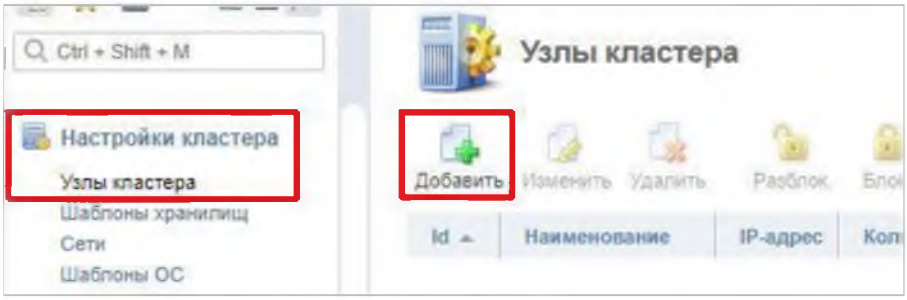


Рисунок 2.36 – Розділ вузла кластеру

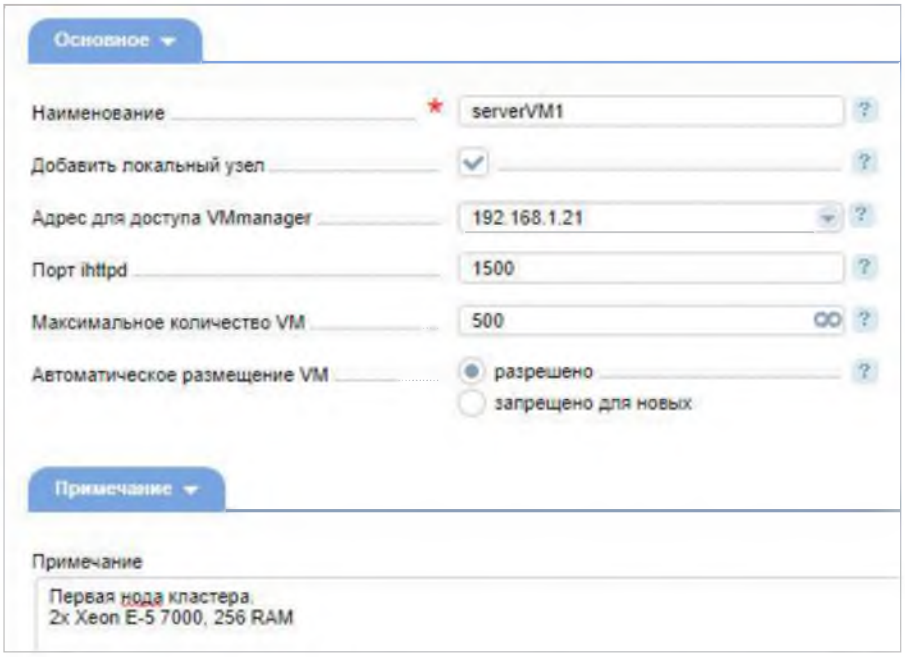


Рисунок 2.37 – Налаштування вузла кластеру,

де найменування - ім'я ноди. Нодою (node - вузол) називається один із групи сервер, об'єднаний у загальний кластер разом із іншими серверами, які також називаються нодами. Об'єднання в кластер проводиться для виконання спільних завдань, з якими не може впоратися окремий сервер [27];

додати локальний вузол — каже про те, що додається локальний сервер;

адреса для доступу VMmanager — IP-адреса, за якою буде доступний сервер;

порт ihttpd – порт для керування;

максимальна кількість VM — кількість машин, що можуть бути створені на сервері;

автоматичне розміщення VM – спосіб автоматичного розміщення віртуальних машин на сервері;

примітка – довільний текст.

10. Після цього потрібно натиснути кнопку «ОК», щоб система встановила необхідні пакети та додала ноду до кластера. Далі необхідно додати шаблони для операційних систем. Для цього потрібно перейти до розділу «Налаштування кластера» та «Шаблони ОС», вибрати бажаний шаблон і натиснути «Встановити», а потім «ОК». Для використання кількох образів, цю дію необхідно повторити для кожного з них. Приклад вікна зображено на рисунку 2.38.

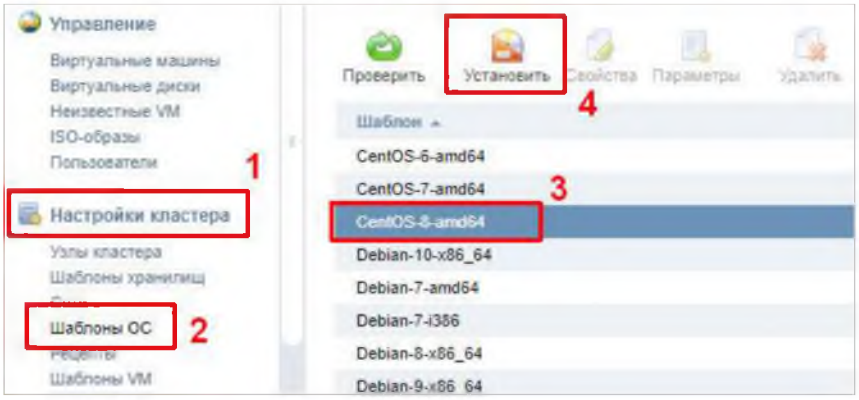


Рисунок 2.38 – Шаблони операційних систем

11. Тепер потрібно створити користувача. Для цього потрібно перейти в розділ «Керування» та «Користувачі», натиснути кнопку «Створити» та заповнити поля для користувача, якого потрібно створити. Приклади вікон зображено на рисунках 2.39 та 2.40.

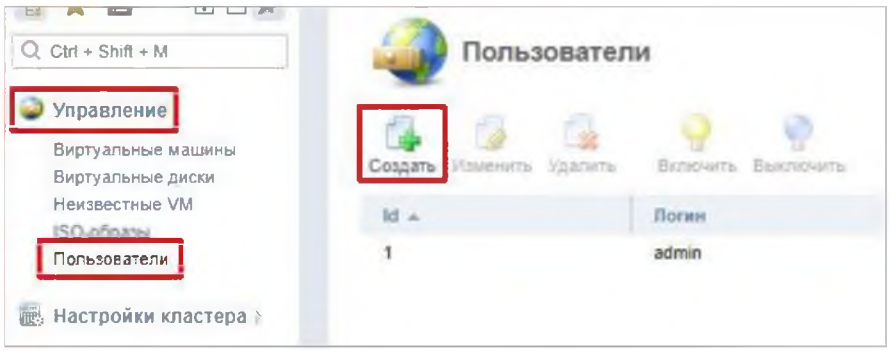


Рисунок 2.39 - Користувачі

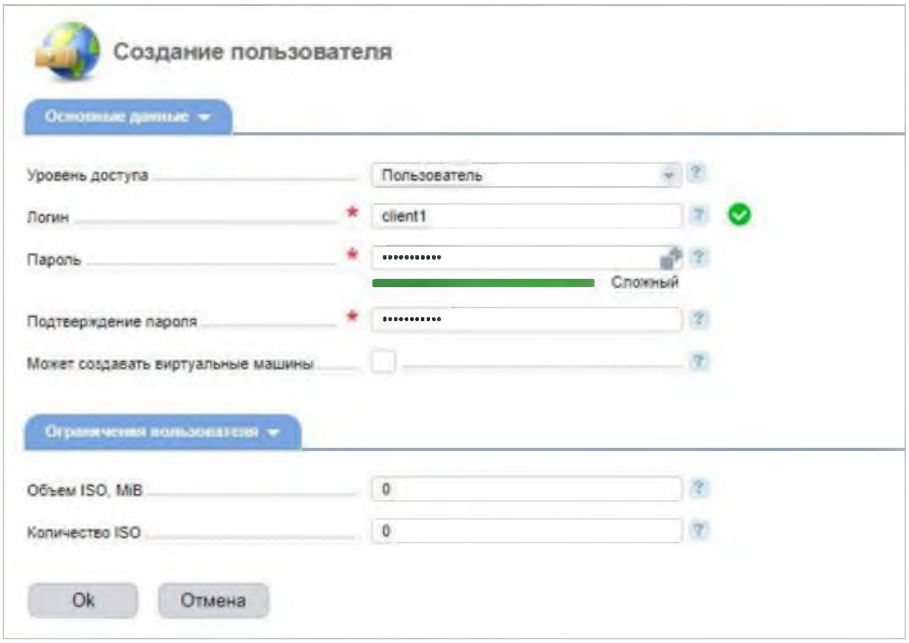


Рисунок 2.40 – Створення користувача,

де рівень доступу — права нового користувача. Це може бути адміністратор чи звичайний користувач;

логін – ім'я облікового запису;

пароль/підтвердження пароля — пароль для облікового запису;

може створювати віртуальні машини – чи дозволено користувачеві створювати віртуальні машини;

об'єм ISO, MiB – обсяг дискового простору під образи. Можна не ставити, якщо заданий у налаштуваннях політик;

кількість ISO — кількість образів, які користувач може додати. Можна не ставити, якщо заданий у налаштуваннях політик.

12. На цьому етапі необхідно створити віртуальну машину. Для цього потрібно перейти в розділ «Керування» та «Віртуальні машини», натиснути кнопку «Створити» та заповнити поля для віртуальної машини, яку потрібно створити. Приклади вікон зображено на рисунках 2.41 та 2.42.

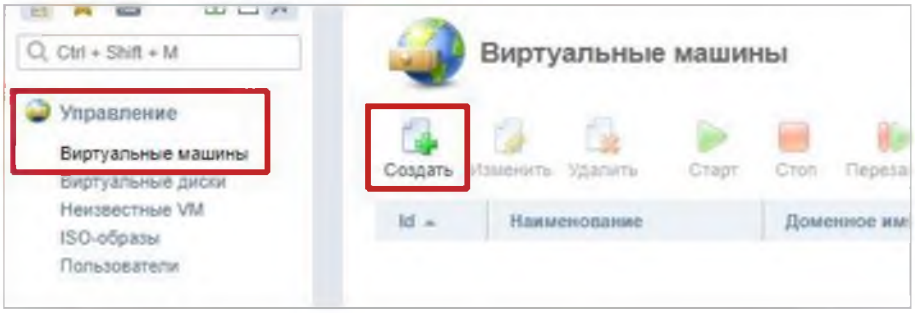


Рисунок 2.41 – Розділ віртуальні машини

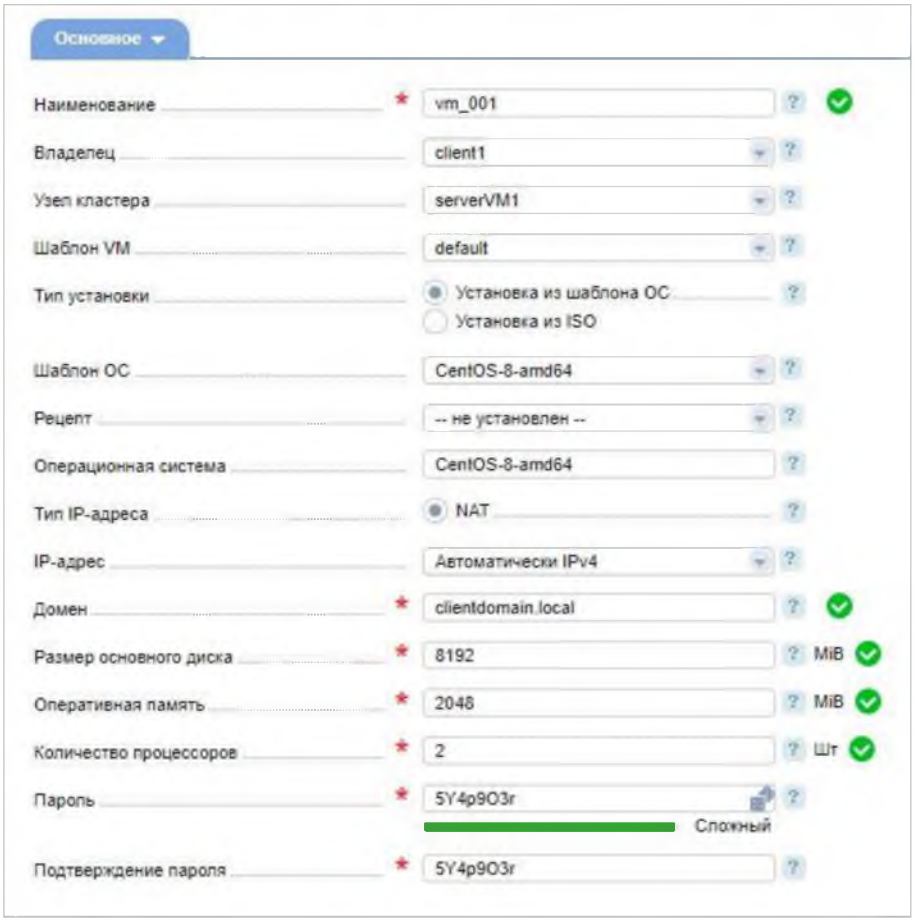


Рисунок 2.42 – Створення віртуальної машини,

де назва – назва для віртуальної машини;

власник - користувач, якому належатиме створювана машина;

вузол кластера - серверна нода кластера, на якому буде створено віртуальну машину;

шаблон VM — шаблон із заготовленими налаштуваннями;

тип установки – як саме встановлювати систему – із готового шаблону або свого образу ISO;

шаблон ОС — це шаблон системи (якщо було обрано відповідний тип установки);

рецепт - після установки системи її можна відразу налаштувати для виконання якогось сервісу;

операційна система - операційна система, що встановлюється. Відповідає вибраному шаблону ОС;

тип IP-адреси – тип адреси. У цьому випадку доступний лише один тип. Усього їх може бути 3 - приватний, публічний та NAT. Можливість вибору залежить від створених мереж;

IP-адреса — спосіб призначення адреси. Автоматично дозволить отримати адресу DHCP;

домен - доменне ім'я для створюваної машини;

розмір основного диска – обсяг дискового простору, який буде виділено віртуальній машині;

оперативна пам'ять – обсяг пам'яті, який буде виділено віртуальній машині;

кількість процесорів – кількість процесорів для створюваної машини;

пароль/підтвердження пароля - пароль для доступу до VNC і користувача root.

13. Тепер необхідно додати додаткові налаштування, після чого створити віртуальну машину. Приклад вікна зображено на рисунку 2.43.

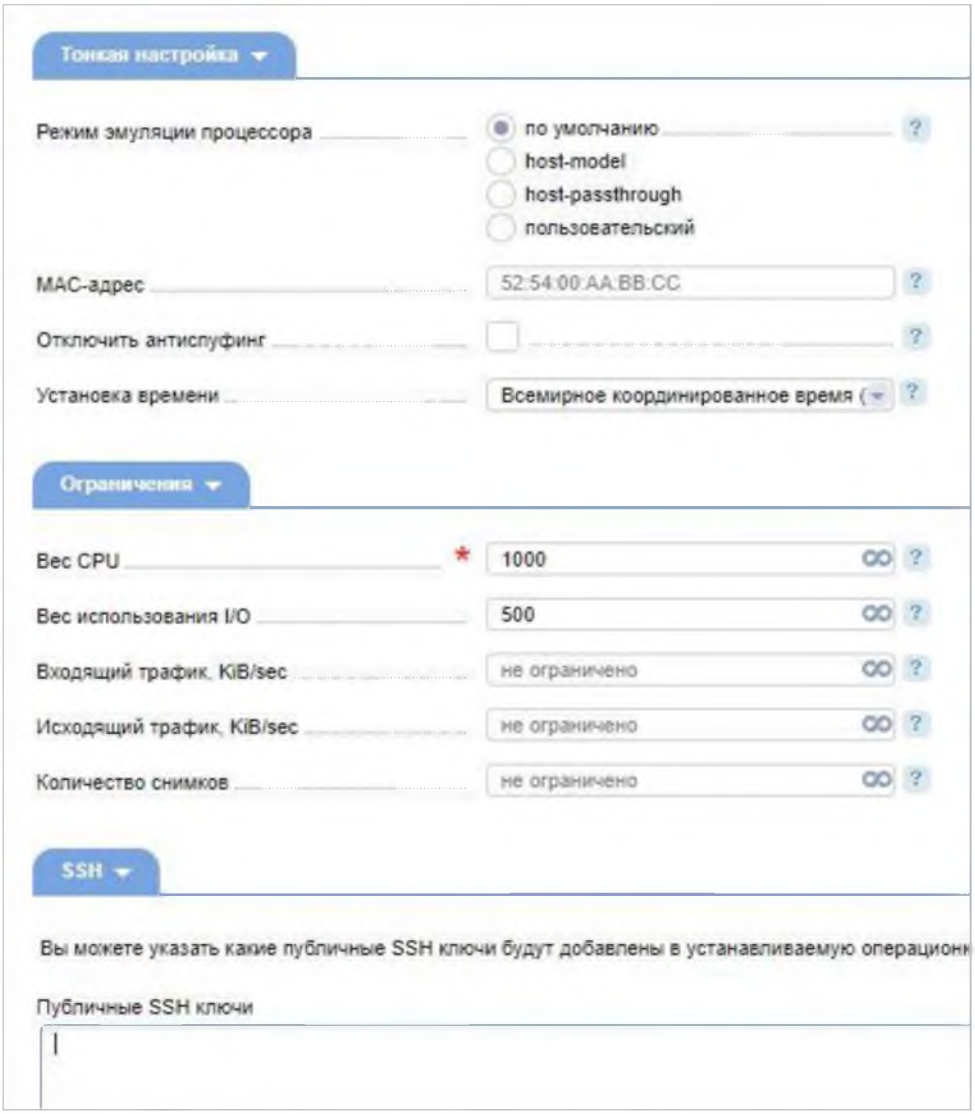


Рисунок 2.43 – Додаткові налаштування,

де режим емуляції процесора – емуляція процесора. За замовчуванням використовується віртуальний процесор QEMU. Під час емуляції в режимі host-model використовується опис процесора, визначений libvirt на основі процесора вузла кластера. У режимі host-passthrough в точності емулюється процесор вузла кластера. Користувацький дозволить задати свої дані про процесор;

MAC-адреса — фізична мережна адреса, яка буде виділена для віртуальної машини;

вимкнути антиспуфінг — відключає можливість створення правил антиспуфінгу (блокування повідомлень, надісланих від локального домену, але неавторизованої IP-адреси);

установка часу — спосіб синхронізації годинника віртуальної машини з годинником сервера;

вага CPU - відносна вага для процесора. У разі нестачі ресурсів, перевага буде віддана тій машині, у якої більша вага CPU;

вага використання I/O — відносна вага дискового сховища. У разі нестачі ресурсів, перевага буде віддана тій машині, у якої більша вага I/O;

вхідний трафік, KiB/sec - обмеження швидкості вхідного трафіку;

вихідний трафік, KiB/sec - обмеження швидкості вихідного трафіку;

кількість знімків — максимально можлива кількість снапшотів, які можна зробити для віртуальної машини;

публічні SSH ключі — якщо є ключі для безпарольного доступу через SSH, потрібно їх занести в дане поле.

Приклад того, як виглядає розділ «Віртуальні машини», в якому доступний перегляд віртуальних машин, швидкі дії та масові операції зображено на рисунку 2.44.

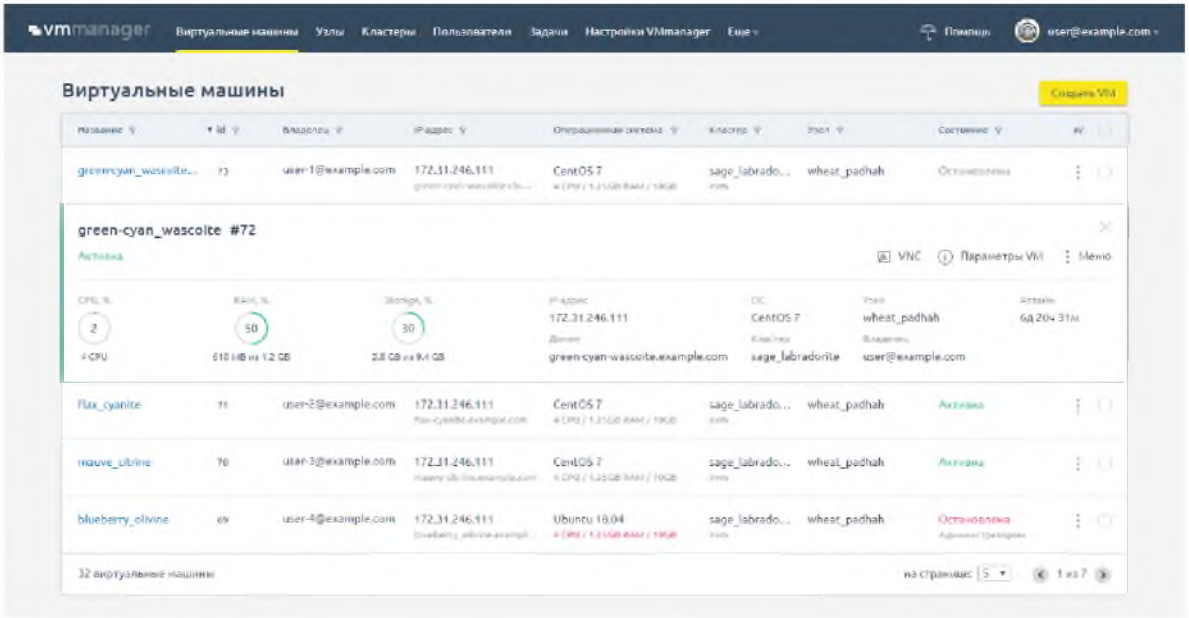


Рисунок 2.44 - Розділ «Віртуальні машини»

2.12.5 Встановлення програмного забезпечення на віртуальній машині

VMmanager може провести автоматичне встановлення потрібних програм на віртуальному робочому столі за допомогою скриптів. Скрипти на

віртуальній машині запускаються одразу після встановлення операційної системи. Щоб написати скрипт, достатньо знання команд bash, з якими знайома більшість системних адміністраторів.

Для установки серверного програмного забезпечення можна використовувати скрипти з репозиторію ISPsystem або створити власні на їх основі.

Корисні скрипти з репозиторію:

- OpenVPN – встановлює VPN-сервер для створення захищених мережевих підключень;

- Teamspeak – встановлює сервер для голосового спілкування, що дозволяє проводити наради з великою кількістю співробітників;

- LAMP – встановлює необхідне ПЗ для підняття публічного або внутрішнього веб-сервера компанії;

- Bitrix Env Crm - встановлює CRM "Бітрікс24";

- Bitrix Env - встановлює комплект ПЗ "1С-Бітрікс: Веб-оточення".

Приклад вікна розділу «Скрипти», в якому можна переглянути всі скрипти, доступні для встановлення на віртуальний сервер, та створити власний зображено на рисунку 2.45.

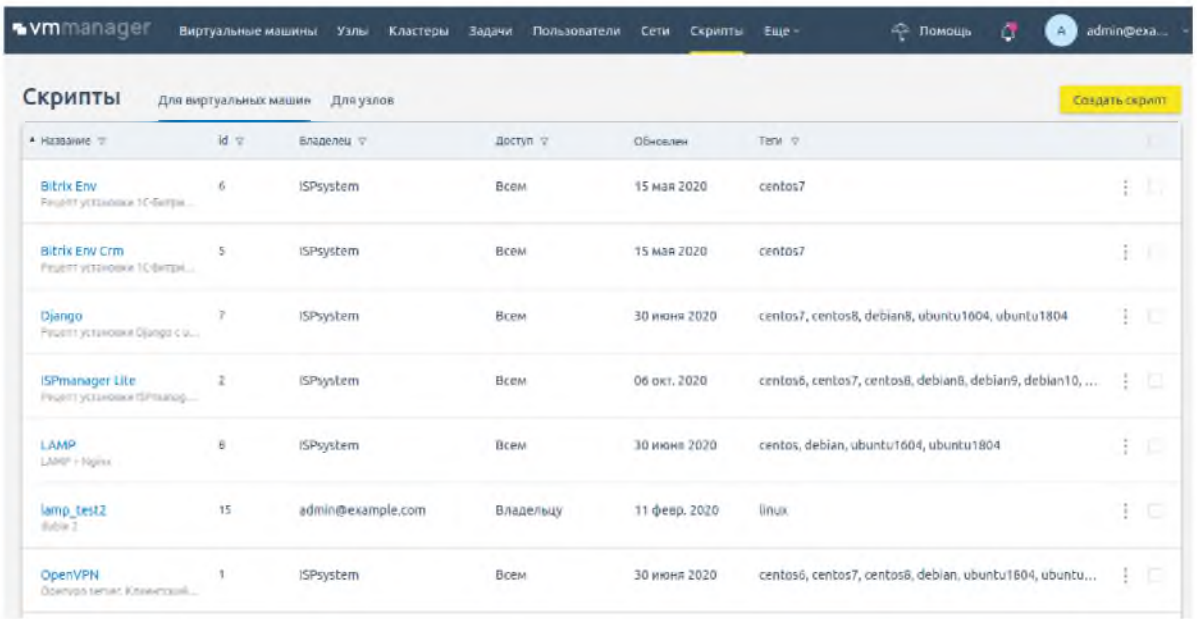


Рисунок 2.45 - Розділ «Скрипти»

2.13 Встановлення VNC-клієнта та підключення до віртуальної машини VMmanager

1. Для початку встановлення необхідно завантажити дистрибутив TightVNC на офіційному сайті за посиланням - [28]. Потім його запустити та натиснути кнопку «Next». Приклад вікна зображено на рисунку 2.46.

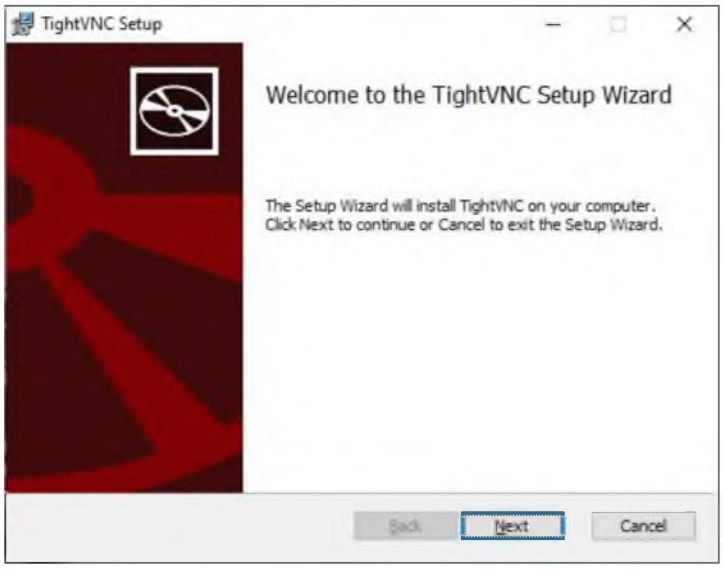


Рисунок 2.46 – Привітальне вікно інсталятора

2. Тепер потрібно ухвалити ліцензійну угоду та натиснути кнопку «Next». Приклад вікна зображено на рисунку 2.47.

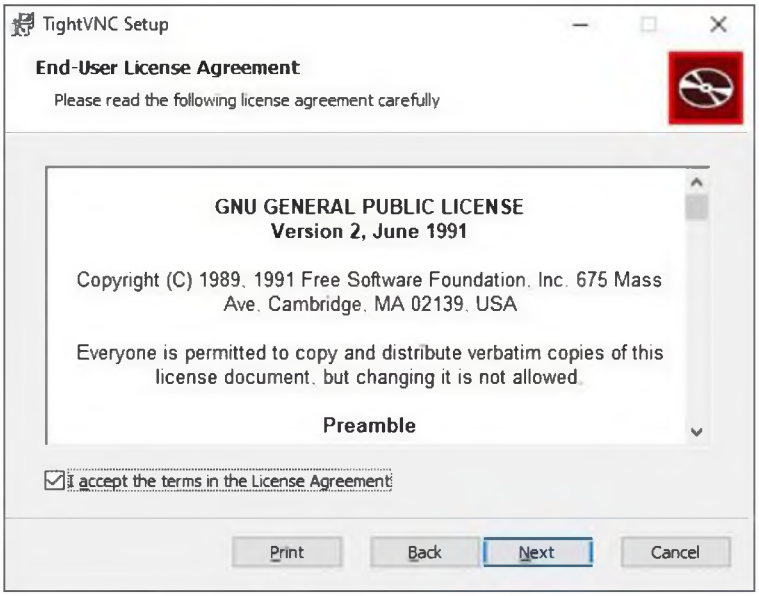


Рисунок 2.47 – Ліцензійні умови

3. У цьому вікні необхідно натиснути кнопку "Custom", потім вибрати TightVNC Server і натиснути "Entire feature will be unavailable", щоб не встановлювати його, після чого натиснути "Next". Приклади вікон зображено на рисунках 2.48 та 2.49.

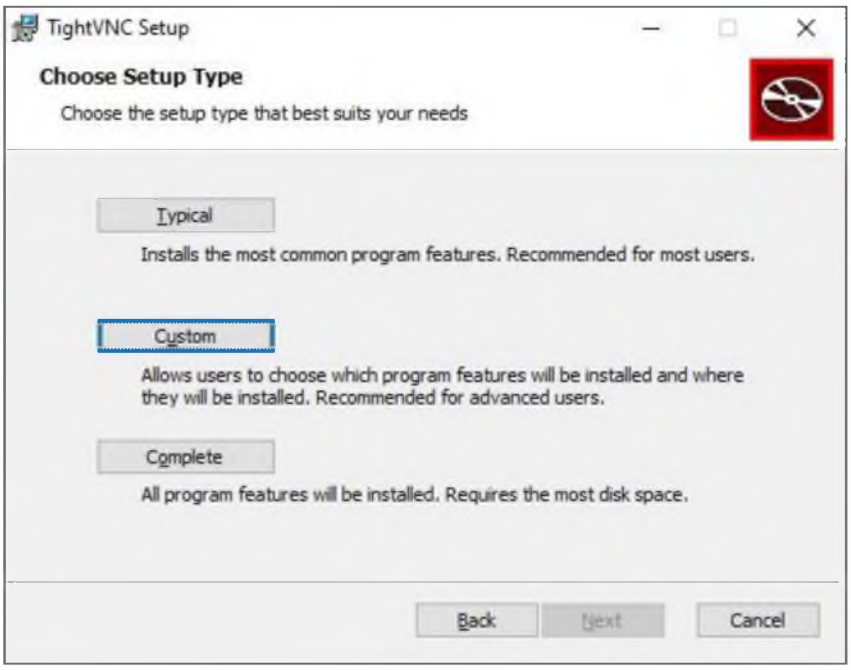


Рисунок 2.48 – Вибір типу встановлення

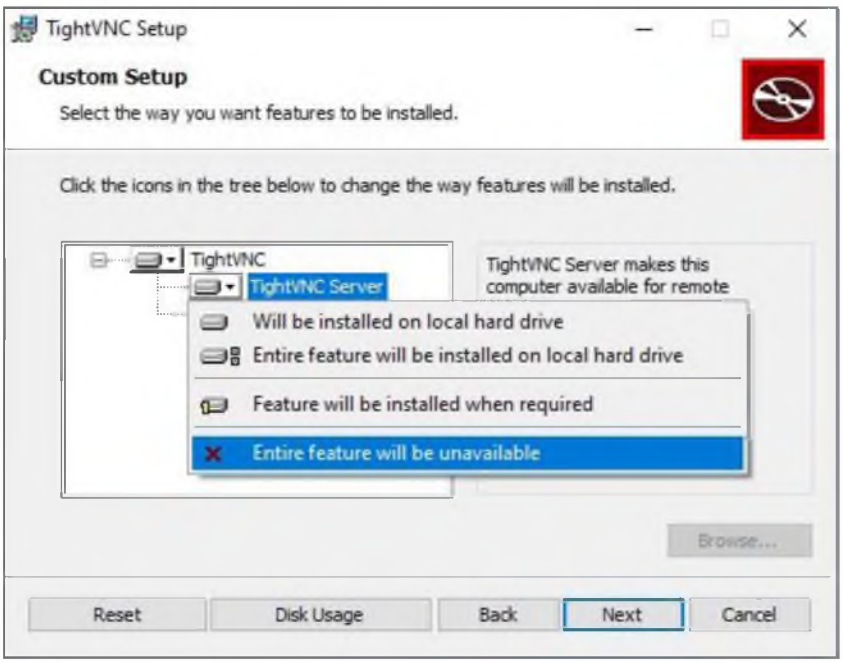


Рисунок 2.49 – Вибір програм для встановлення

4. Тепер необхідно активувати пункт «Associate .vnc files with TightVNC Viewer», якщо він ще не активний, та натиснути кнопку «Next». Потім «Install», дочекатися закінчення установки та натиснути кнопку «Finish». Приклади вікон зображено на рисунках 2.50, 2.51, 2.52 та 2.53.

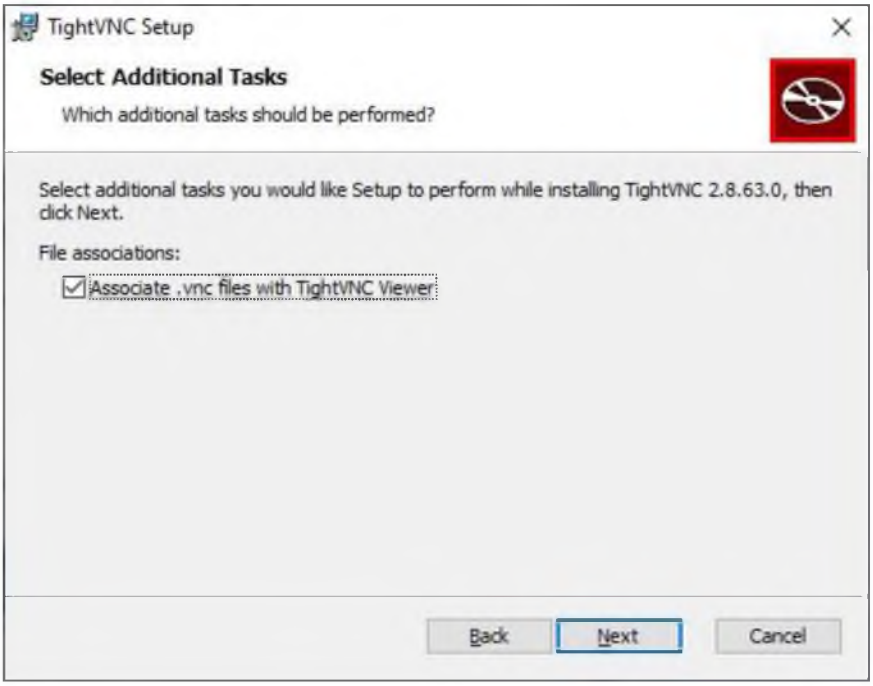


Рисунок 2.50 – Вибір додаткових можливостей

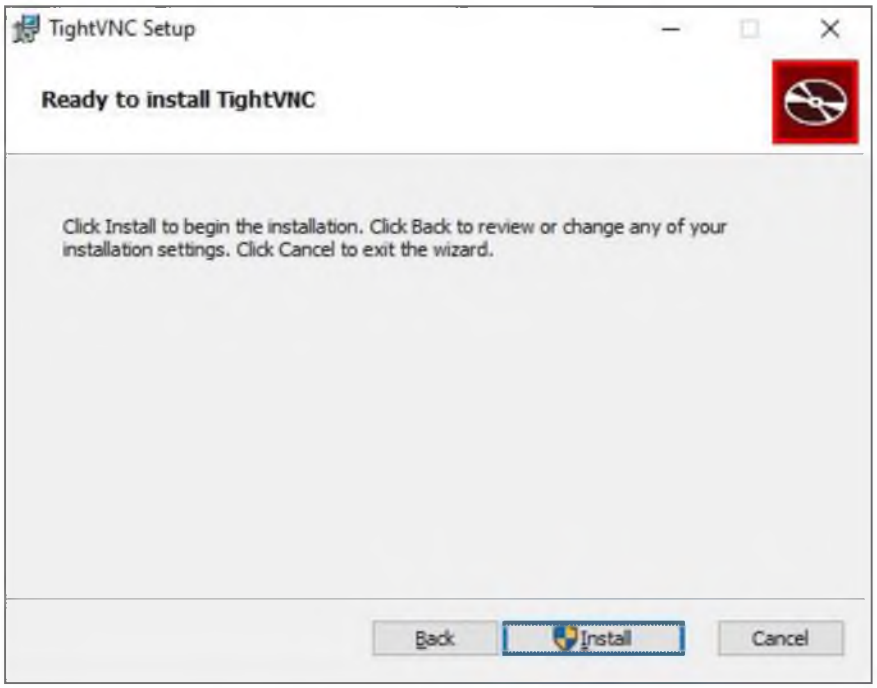


Рисунок 2.51 – Запрошення до встановлення

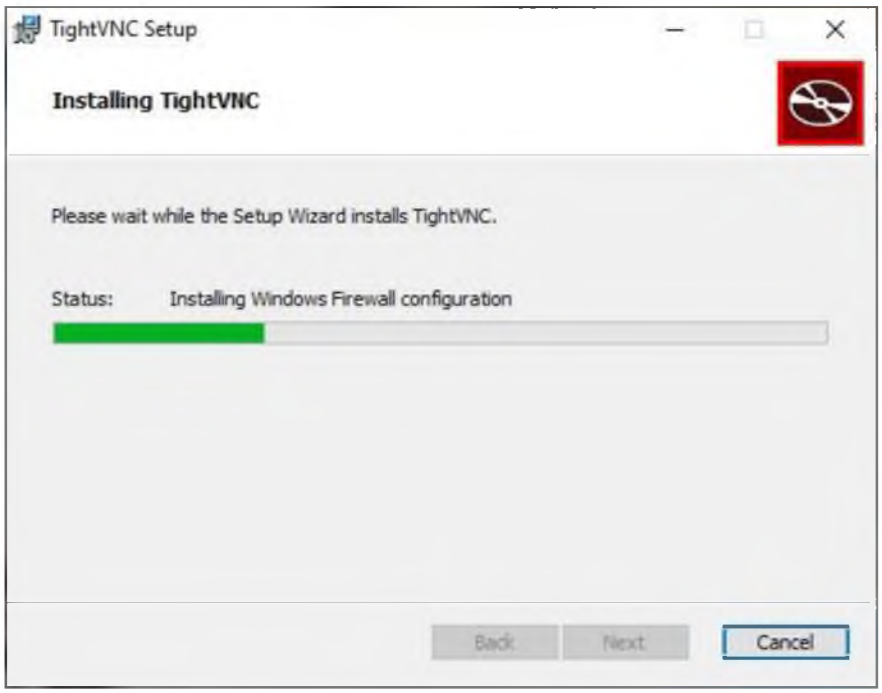


Рисунок 2.52 – Статус встановлення

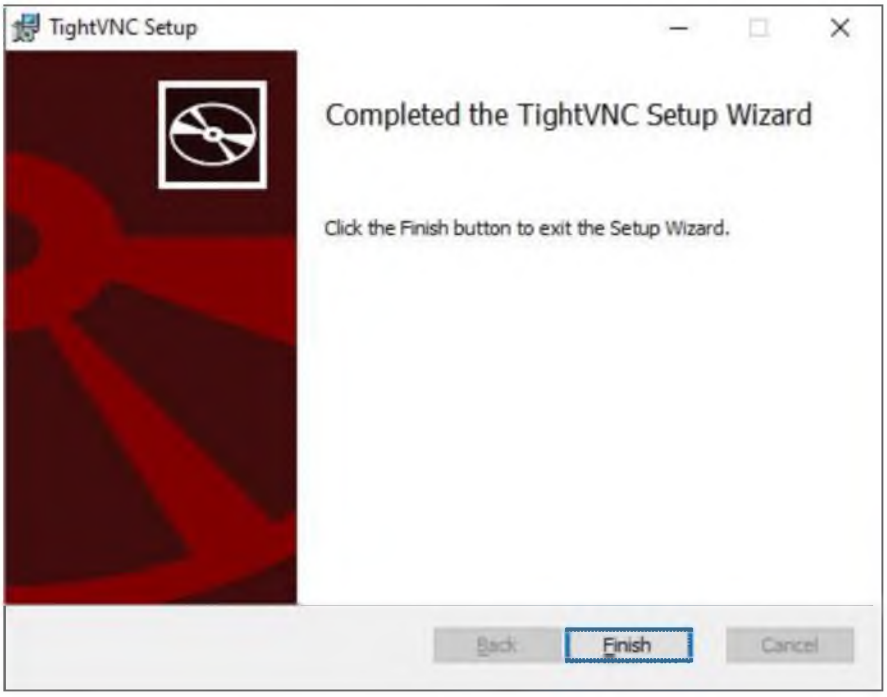


Рисунок 2.53 – Вікно завершення встановлення

5. На цьому етапі необхідно отримати дані, які використовуються для підключення до віртуальної машини VNC. Вони вказані на сторінці віртуальної машини у розділі «Віртуальні машини». Після переходу в розділ необхідно

натиснути "Параметри VM", а потім "Налаштування VNC". Звідси необхідно отримати дані для підключення, а саме:

- адреса сервера VNC;
- порт для підключення до сервера VNC;
- пароль для підключення до сервера VNC. [20]

6. Далі необхідно запустити TightVNC Viewer, ввести в поле «Remote Host» адресу сервера VNC та порт для підключення до сервера VNC, натиснути «Connect» і в наступному вікні ввести пароль для підключення до сервера VNC. Таким чином, буде отримано доступ до віддаленого робочого столу. Приклади вікон зображено на рисунках 2.54, 2.55 та 2.56.

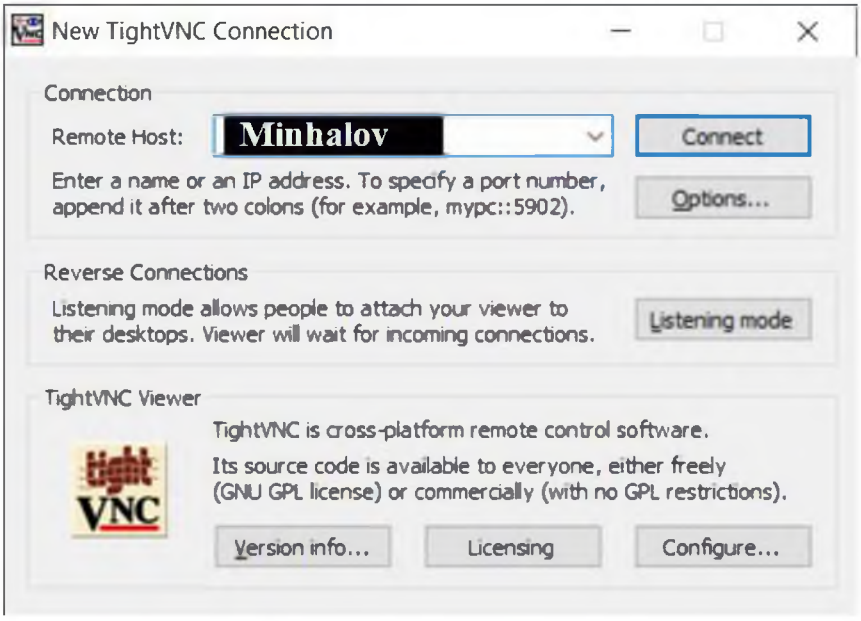


Рисунок 2.54 – Вікно налаштування підключення до серверу VNC

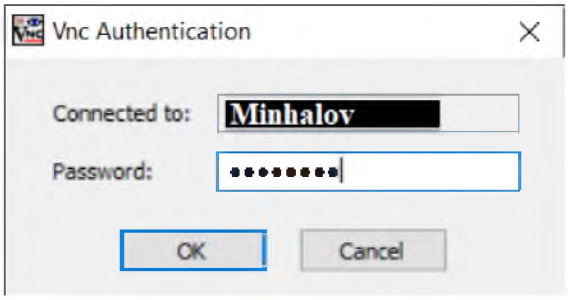


Рисунок 2.55 – Вікно вводу паролю

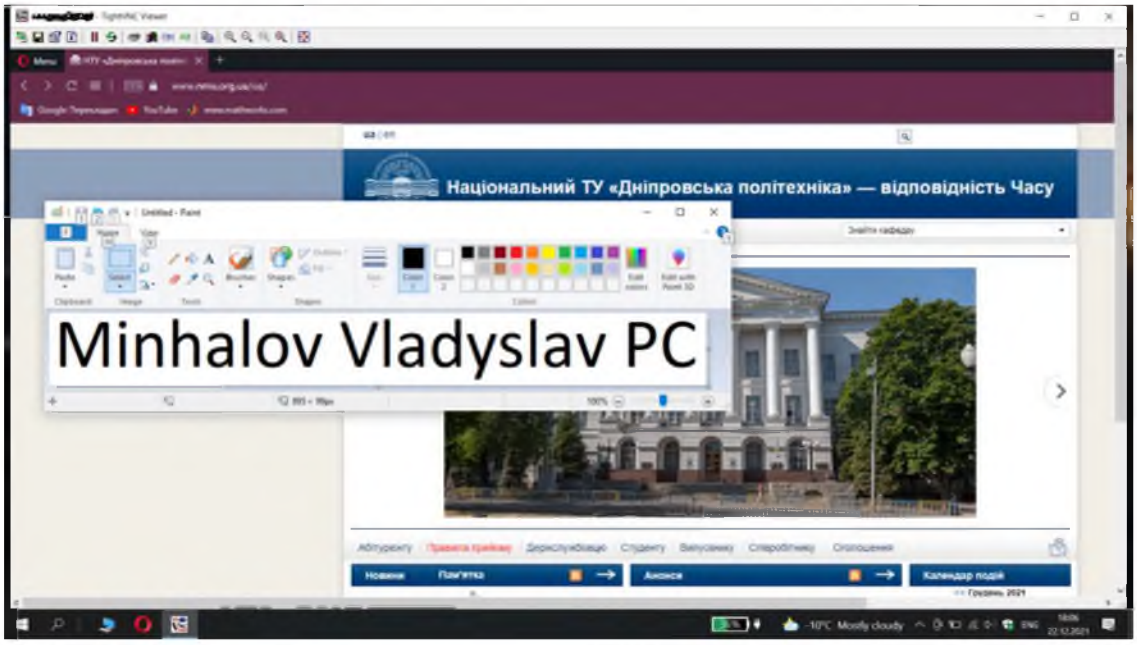


Рисунок 2.56 – Вікно робочого столу віртуальної машини, до якої було виконано підключення

2.14 Курси з кібербезпеки

Крім програмно-апаратних методів захисту, необхідно мати документально-організаційні, які будуть розглянуті нижче.

Після ознайомлення співробітника з політиками безпеки компанії необхідно перевірити, наскільки добре він запам'ятав і зрозумів пройдений матеріал. Це можливо виконати, наприклад, шляхом проходження курсів з кібербезпеки компанії кожні півроку/рік використовуючи, наприклад:

- спрощений переказ політики безпеки з можливістю повністю з нею ознайомитися через спеціально залишене для цього посилання. Приклад зображено на рисунку 2.57;

- тестування з різними варіантами відповіді (чекбокси, ситуації). Приклади зображено на рисунках 2.58 та 2.59;

- ситуації. Приклад ситуації зображено на рисунку 2.60.

Надійний пароль

Дуже важливо вигадувати складні паролі, що складаються з букв (великих і малих), цифр та символів.

Не використовуйте один пароль для різних онлайн сервісів! Якщо зловмисник отримає дані облікового запису для одного сервісу, то, напевно, спробує отримати доступ і до інших користуючись вже відомими даними.

Придумайте алгоритм побудови пароля. Наприклад:
1. Поточний день тижня;
2. Суть ресурсу, у якому реєструєтесь.
3. Поєднайте їх в одне слово;
4. Замініть деякі літери на символи;
5. Використовуйте різний регістр для літер;
6. Додайте наприкінці кожного слова цифри.

Приклад:
1. Понеділок;
2. Продажі
3. ПонеділокПродажі
4. Пон/д!локПр*д@жі
5. пОн/Д!локПр*д@жі
6. пОн/Д!лок67Пр*д@жі89

Ознайомтеся з парольною політикою компанії за цим посиланням.

Рисунок 2.57 – Ознайомлення з парольною політикою компанії

Які з паролів є більш безпечними?

- [ ] 15102000
- [ ] Червоний
- [x] *(sdj2k:!Wt
- [ ] chervoniy
- [x] і(л3д"1івКр

Рисунок 2.58 – Декілька правильних відповідей

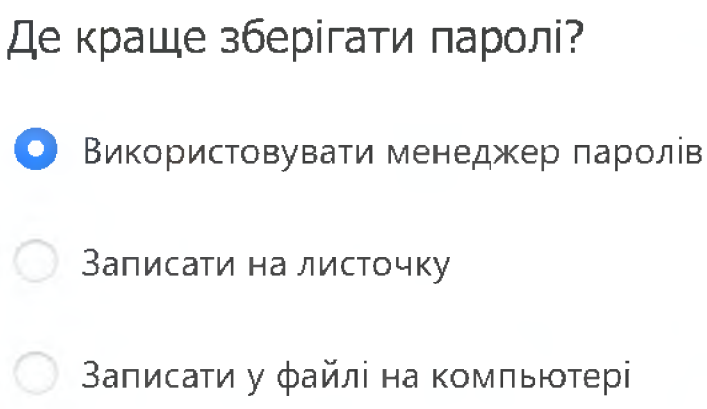


Рисунок 2.59 – Одна правильна відповідь

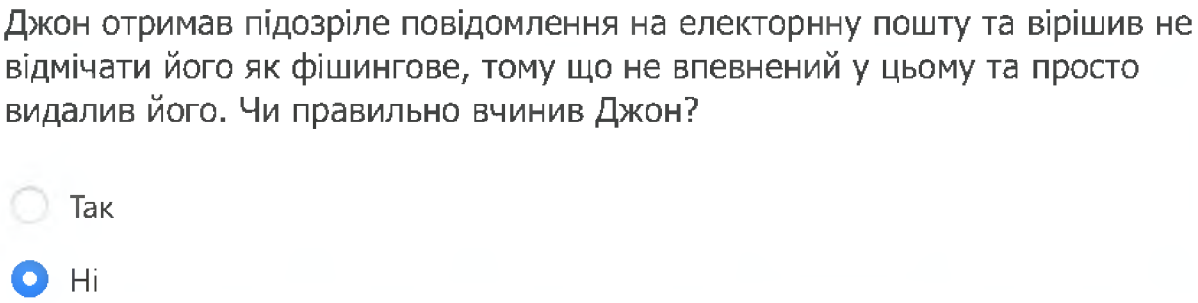


Рисунок 2.60 – Ситуація

2.15 Розробка політики безпеки інформації

2.15.1 Політика «чистого столу»

1. Мета

Метою цієї політики є встановлення мінімальних вимог щодо підтримки «чистого столу» - де конфіденційна інформація про наших співробітників, нашу інтелектуальну власність, наших клієнтів та наших постачальників захищена у замкнених місцях та поза сайтом.

2. Сфера застосування

Ця політика поширюється на всіх співробітників підприємства та їх філій.

3. Політика

3.1 Співробітники зобов'язані гарантувати, що вся конфіденційна інформація в твердій копії або в електронній формі буде захищена на робочому місці в кінці робочого дня і коли очікується їх тривала відсутність.

3.2 Робочі станції комп'ютера повинні бути заблоковані, коли робоча область незайнята.

3.3 Робочі станції комп'ютера повинні бути повністю вимкнені наприкінці робочого дня.

3.4 Ноутбуки повинні бути або заблоковані замикаючим кабелем, або зафіксовані у шухляді.

3.5 Паролі не можуть залишатися на наклеєних нотатках, розміщених на комп'ютері або під ними, а також не можуть бути записані у доступному місці.

3.6 Роздруківки, що містять інформацію з інформацію з обмеженим доступом, слід негайно видалити з принтера.

3.7 Документи, що містять інформацію з обмеженим доступом, після утилізації повинні бути подрібнені за допомогою подрібнювачів або поміщені в секретні контейнери для захоронення.

3.8 Дошки, що містять інформацію з обмеженим доступом, слід очистити.

3.9 Портативні обчислювальні пристрої, такі як ноутбуки та планшети, повинні бути заблоковані у разі їх залишення без нагляду.

Усі принтери та факсимільні машини повинні бути очищені від паперів, як тільки вони надруковані; це допомагає гарантувати, що конфіденційні документи не залишаються в лотках для принтерів, щоб невірна особа підняла.

4. Дотримання політики

4.1 Відповідальність

Відповідальним за дотримання політики безпеки є системний адміністратор підприємства.

4.2 Винятки

Будь-який виняток із політики повинен бути затверджений з керівництвом підприємства та системним адміністратором заздалегідь.

4.3 Недотримання

Працівник, який виявив порушення цієї політики, може зазнати дисциплінарного стягнення, аж до припинення роботи.

2.15.2 Політика електронної пошти

1 Мета

Метою цієї політики електронної пошти є забезпечення належного використання системи електронної пошти підприємства та інформування користувачів про те, що підприємство вважає прийнятним та неприйнятним для використання його системи електронної пошти. Ця політика визначає мінімальні вимоги щодо використання електронної пошти в мережі підприємства.

2 Сфера застосування

Ця політика охоплює належне використання будь-якого електронного листа, надісланого з електронної адреси підприємства та стосується всіх співробітників, продавців та агентів, що працюють від імені підприємства.

3 Політика

3.1 Будь-яке використання електронної пошти повинно відповідати політиці підприємства та процедурам етичної поведінки, безпеки, дотримання чинного законодавства та належної ділової практики.

3.2 Обліковий запис електронної пошти підприємства слід використовувати насамперед для цілей, пов’язаних з бізнесом; особисте спілкування дозволено обмежено, але комерційне використання, яке не стосується підприємства, заборонено.

3.3 Усі дані підприємства, що містяться в електронному повідомленні або вкладеному файлі, повинні бути захищені відповідно до стандарту захисту даних.

3.4 Електронний лист, ідентифікований як підприємство, що містить діловий запис зберігається відповідно до графіку зберігання записів підприємства.

3.5 Система електронної пошти підприємства не повинна використовуватися для створення або розповсюдження будь-яких зривних або образливих повідомлень, включаючи образливі коментарі щодо раси, статі, кольору волосся, інвалідності, віку, сексуальної орієнтації, порнографії, релігійних та політичних переконань, чи національного походження. Співробітники, які отримують будь-які електронні листи з цим вмістом від будь-якого співробітника підприємства, повинні негайно повідомити про це своєму керівнику.

3.6 Користувачам забороняється автоматично пересилати електронну пошту підприємства сторонній системі електронної пошти (зазначено в 3.7 нижче). Окремі повідомлення, які пересилаються користувачем, не повинні містити конфіденційну інформацію підприємства.

3.7 Користувачам забороняється користуватися сторонніми системами електронної пошти та серверами зберігання даних, такими як Google, Yahoo та MSN Hotmail тощо, для ведення бізнесу підприємства, створення або запам'ятовування будь-яких зобов'язальних операцій, а також зберігання або збереження електронної пошти від імені підприємства. Такі комунікації та транзакції повинні проводитись через належні канали, використовуючи підтверджену документацію підприємства.

3.8 Використання розумної кількості ресурсів підприємства для особистих електронних листів є прийнятним, але повідомлення, що не стосується роботи, зберігається в окремій папці, пов'язаній з роботою електронної пошти. Надсилання ланцюга листів або жартівливих листів із облікового запису підприємства заборонено.

3.9 Працівники підприємства не повинні очікувати конфіденційності всього, що вони зберігають, надсилають або отримують у системі електронної пошти компанії.

3.10 Підприємство може контролювати повідомлення без попереднього повідомлення. Підприємство не зобов'язано контролювати електронні повідомлення.

4 Дотримання політики

4.1 Відповідальність

Відповідальним за дотримання політики безпеки є системний адміністратор підприємства.

4.2 Винятки

Будь-який виняток із політики повинен бути затверджений з керівництвом підприємства та системним адміністратором заздалегідь.

4.3 Недотримання

Працівник, який виявив порушення цієї політики, може зазнати дисциплінарного стягнення, аж до припинення роботи.

2.15.3 Політика захисту пароля

1. Мета

Метою цієї політики є встановлення стандарту створення надійних паролів та захисту цих паролів.

2. Сфера застосування

Сфера дії цієї політики включає весь персонал, який має або несе відповідальність за обліковий запис будь-якої системі, яка знаходиться в будь-якому об'єкті підприємства та має доступ до мережі підприємства.

3. Політика

3.1 Створення пароля

3.1.1 Користувачі повинні використовувати окремий унікальний пароль для кожного свого облікового запису. Користувачі не можуть використовувати паролі, пов’язані з роботою, для власних особистих акаунтів.

3.1.2 Облікові записи користувачів, які мають привілеї на системному рівні, повинні мати унікальний пароль від усіх інших облікових записів, що зберігаються цим користувачем для доступу до привілеїв на рівні системи.

3.2 Зміна пароля

3.2.1 Паролі слід змінювати лише тоді, коли є підстави вважати, що пароль порушений.

3.3 Захист паролем

3.3.1 Паролі не повинні нікому розповсюджуватися, включаючи керівників та співробітників. Всі паролі слід розглядати як конфіденційну інформацію підприємства.

3.3.2 Паролі не можна вставляти в електронні повідомлення чи інші форми електронного зв'язку і розкривати комусь по телефону.

3.3.3. Паролі можуть зберігатися лише у «адміністраторів паролів», уповноважених організацією.

3.3.4 Не використовуйте функцію "Запам'ятати пароль" програм.

3.3.5 Будь-який користувач, який підозрює, що його пароль може бути порушений, повинен повідомити про інцидент та змінити всі паролі.

4.1 Відповідальність

Відповідальним за дотримання політики безпеки є системний адміністратор підприємства.

4.2 Винятки

Будь-який виняток із політики повинен бути затверджений з керівництвом підприємства та системним адміністратором заздалегідь.

4.3 Недотримання

Працівник, який виявив порушення цієї політики, може зазнати дисциплінарного стягнення, аж до припинення роботи.

2.15.4 Політика безпеки сервера

1. Мета

Метою цієї політики є встановлення стандартів базової конфігурації внутрішнього серверного обладнання, яким володіє та керує підприємство. Ефективна реалізація цієї політики дозволить мінімізувати несанкціонований доступ до власницької інформації та технологій підприємства.

2. Сфера застосування

Усі працівники, підрядники, консультанти, тимчасові та інші працівники підприємства та його філій повинні дотримуватися цієї політики. Ця політика поширюється на серверне обладнання, яке перебуває у власності.

Ця політика визначає вимоги до обладнання у внутрішній мережі підприємства.

3. Політика

3.2 Вимоги до конфігурації

3.2.1 Конфігурація операційної системи повинна відповідати затвердженим інструкціям підприємства.

3.2.2 Служби та додатки, які не використовуються, повинні бути відключені, де це можливо.

3.2.3 Доступ до сервісів повинен реєструватися та / або захищатися методами контролю доступу, такими як брандмауер веб-додатків, якщо це можливо.

3.2.4 Найновіші оновлення безпеки повинні бути встановлені в системі якнайшвидше, єдиний виняток - коли негайне застосування заважає бізнес-вимогам.

3.2.5 Довірчі відносини між системами є ризиком для безпеки, і їх слід уникати. Не використовуйте довірчі відносини, коли якийсь інший спосіб спілкування є достатнім.

3.2.6 Завжди використовуйте стандартні принципи безпеки з найменш необхідним доступом для виконання функції. Не використовуйте root, коли буде зроблено непривілейований обліковий запис.

3.2.7 Сервери повинні бути фізично розташовані в середовищі з контролем доступу.

3.2.8 Серверам спеціально забороняється працювати з неконтрольованих приміщень кабіни.

3.2.9 Усі події, пов’язані з безпекою на критичних системах, повинні реєструватися,

4. Дотримання політики

4.1 Відповідальність

Відповідальним за дотримання політики безпеки є системний адміністратор підприємства.

4.2 Винятки

Будь-який виняток із політики повинен бути затверджений з керівництвом підприємства та системним адміністратором заздалегідь.

4.3 Недотримання

Працівник, який виявив порушення цієї політики, може зазнати дисциплінарного стягнення, аж до припинення роботи.

2.15.5 Антивірусна політика

1. Мета

Ця політика спрямована на те, щоб запобігти зараженню комп'ютерних вірусів та іншого шкідливого коду комп'ютерів та комп'ютерних систем підприємства. Ця політика покликана запобігти пошкодженню програм, даних, файлів та апаратних засобів користувачів.

2. Сфера застосування

Ця політика поширюється на всіх працівників підприємства та його філій повинні дотримуватися цієї політики.

3. Політика

3.1 Завжди завантажуйте та використовуйте лише ліцензоване ПЗ.

3.2 Ніколи не відкривайте файли, приєднані до електронного листа з невідомого, підозрілого чи недостовірного джерела. Видаліть ці вкладені файли негайно, а потім "подвійно видаліть", видаливши кошик.

3.3 Видаліть спам, ланцюжок та інші непотрібні електронні листи без переадресації.

3.4 Ніколи не завантажуйте файли з невідомих або підозрілих джерел.

3.5 Уникайте прямого обміну дисками з доступом до читання / запису, якщо для цього не існує абсолютно ділових вимог.

3.6 Завжди скануйте зовнішні носії з невідомого джерела на наявність вірусів перед її використанням.

3.7 Регулярно створюйте резервні копії критичних даних та конфігурацій системи та зберігайте їх у безпечному місці.

3.9 Нові віруси виявляються майже щодня. Періодично перевіряйте антивірус на наявність оновлень.

4. Дотримання політики

4.1 Відповідальність

Відповідальним за дотримання політики безпеки є системний адміністратор підприємства.

4.2 Винятки

Будь-який виняток із політики повинен бути затверджений з керівництвом підприємства та системним адміністратором заздалегідь.

4.3 Недотримання

Працівник, який виявив порушення цієї політики, може зазнати дисциплінарного стягнення, аж до припинення роботи.

2.15.6 Політика резервного копіювання

1. Мета

Метою цієї політики є надання засобів для відновлювання цілісності комп'ютерних систем у разі відмови апаратного / програмного забезпечення або фізичних катастроф та забезпечення міри захисту від помилок людини або ненавмисного видалення важливих файлів.

2. Сфера застосування

Ця політика поширюється на системного адміністратора підприємства.

3. Політика

Періодично створюється резервна копія всієї інформації на рівні користувача та на рівні комп'ютерної системи підприємства. Резервні носії зберігаються з достатнім захистом та належними умовами навколишнього середовища.

Частота та обсяг резервного копіювання повинні відповідати важливості інформації та прийнятному ризику, визначеному власником даних.

Процес резервного копіювання та відновлення інформаційних ресурсів для кожної системи повинен бути задокументований та періодично переглядатися.

Фізичні засоби доступу, що реалізуються в місцях зберігання резервних копій, повинні відповідати або перевищувати фізичні засоби контролю вихідних систем. Додатково носії резервного копіювання повинні бути захищені відповідно до найвищого рівня чутливості інформації, що зберігається.

Резервні копії операційних систем та іншого програмного забезпечення з важливою інформаційною системою не повинні зберігатися в тому самому місці, що і операційне програмне забезпечення.

Інформація про резервне копіювання системи повинна забезпечуватися захистом від несанкціонованих змін та екологічних умов.

Резервні копії повинні періодично перевірятися, щоб гарантувати їх відновлення. Для підтвердження надійності носія та цілісності інформації резервну інформацію слід перевірити з певною частотою.

Резервна інформація повинна вибірково використовуватися для відновлення функцій інформаційної системи як частини процесу безперервності бізнесу.

Стрічки резервного копіювання повинні мати як мінімум такі ідентифікаційні критерії, які можна легко ідентифікувати за мітками та / або системою штрихового кодування:

- Назва системи
- Дата створення
- Класифікація чутливості
- Контактна інформація

4. Дотримання політики

4.1 Відповідальність

Відповідальним за дотримання політики безпеки є адміністратор безпеки підприємства.

4.2 Винятки

Будь-який виняток із політики повинен бути затверджений з керівництвом підприємства та системним адміністратором заздалегідь.

4.3 Недотримання

Працівник, який виявив порушення цієї політики, може зазнати дисциплінарного стягнення, аж до припинення роботи.

2.16 Оцінка існуючого стану захищеності

ІТС, яка буде використовуватись у віддаленому режимі роботи буде багатокористувачева та розподілена, тому вважається АС 3 класу. Виходячи з цього було обрано профіль захищеності 3.КЦД.1.

Подана ІТС є багатокористувачева та розподілена, тому відноситься до АС 3 класу і враховуючи це було обрано стандартний профіль захищеності 3.КЦД.1:

{ КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

Таблиця 2.7 – Критерії функціонального профіля захищеності

Критерії	Вимоги	Реалізація
КД-2 Базова довірча конфіденційність. Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів.	Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься; КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта; Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта; КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта;	Реалізована. Користувачі мають атрибути доступу до захищеного об’єкта, що належить його домену та можуть визначати користувачів, які будуть мати право на доступ до захищеного об’єкту.

Продовження таблиці 2.7

Критерії	Вимоги	Реалізація
КО-1 Повторне використання об'єктів. Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.	Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС; Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані; Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.	Частково реалізована. На звільненому об’єкті інформація або процес стає недосяжним, але щоб гарантувати це, адміністратор може скористатися командною строкою та виконати команду taskkill, яка завершує процес, який не може завершити «Диспетчер завдань».
КВ-1 Мінімальна конфіденційність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.	Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься; Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності; КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.	Реалізована. При обміні між процесами операційної системи, за допомогою служб якої, використовується буфер обміну - окрема ділянка пам'яті, у яку поміщається інформація при її копіюванні з одного процесу, щоб помістити її в інший. Процеси при обміні інформації не взаємодіють між собою безпосередньо.

Продовження таблиці 2.7

Критерії	Вимоги	Реалізація
ЦД-1 Мінімальна довірча цілісність. Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.	Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься; КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта; Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта; КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт; Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.	Реалізована. Операційна система Windows здійснює розмежування доступу за допомогою розділу «Безпека» у властивостях документів, які обробляються в ІТС підприємства. Також запити на зміну прав доступу до документів обробляються системою на підставі атрибутів доступу користувача.
ЦО-1 Обмежений відкат. Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану.	Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься; Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.	Реалізована. Авторизованому користувачу або процесу дозволено відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу за допомогою снапшотів віртуальних машин через VMmanager.

Продовження таблиці 2.7

Критерії	Вимоги	Реалізація
ЦВ-1 Мінімальна цілісність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.	Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності; КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається.	Не реалізована. Це можна реалізувати за допомогою засобу Microsoft Office, натиснувши кнопку «Файл», потім «Відомості», далі «захист документа» та обравши пункт меню «додати цифровий підпис».
ДР-1 Квоти. Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.	Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься; Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу; Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.	Реалізована. Системний адміністратор обмежив для кожного користувача дисковий простір та конфігурацію усієї ОС та ВМ за допомогою VMmanager.

Продовження таблиці 2.7

Критерії	Вимоги	Реалізація
ДВ-1 Ручне відновлення. Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.	Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС; Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.	Частково реалізована. Після відмови КС або переривання обслуговування КЗЗ адміністратор може скористатися особливим запуском системи у «безпечному режимі» та відновити нормальне функціонування КС або скористатись снапшотами віртуальної машини через VMmanager.
НР-2 Захищений журнал. Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.	Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються; КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки; Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події; КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування; Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.	Реалізована. За допомогою вбудовано засобу Windows «журнал подій», КЗЗ здатен здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Також завдяки VMmanager'у адміністратор має можливість відстежувати поточний статус ВМ та збирати статистику використання ресурсів.

Продовження таблиці 2.7

Критерії	Вимоги	Реалізація
НИ-2 Одиночна ідентифікація і автентифікація. Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.	Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ; Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму; КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.	Реалізована. У кожного користувача КС є свій обліковий запис, за допомогою механізмів якого реалізовано можливість ідентифікації (логін облікового запису) та автентифікувати (пароль облікового запису) користувача для підключення до серверу через VNC клієнт користувача.
НК-1 Однонаправлений достовірний канал. Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.	Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ; Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.	Реалізована. Користувачі отримують доступ до захищеного об’єкту використовуючи клавіатуру та комп’ютерну мишку.

Продовження таблиці 2.7

Критерії	Вимоги	Реалізація
НО-2 Розподіл обов'язків адміністраторів. Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.	Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції; Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі; Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.	Не реалізована. Для того, щоб реалізувати дану послугу, необхідно покласти додаткові обов’язки адміністратора безпеки на іншого працівника підприємства, або найняти нового. Було прийнято рішення покласти ці обов’язки на адміністратора магазину.
НЦ-2 КЗЗ з гарантованою цілісністю. Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.	Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів; КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування; Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.	Реалізовано. Операційна система Windows Server підтримує домен свого власного виконання використовуючи мережевий екран «Брандмауер» та VMmanager налаштовує VPN для підключення до серверу.

Продовження таблиці 2.7

Критерії	Вимоги	Реалізація
НТ-2 Самотестування при старті. Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.	Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ; КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження.	Реалізовано. КЗЗ проводить самотестування при старті за допомогою програми «Power-On self-test». POST складається з послідовних кроків, спрямованих на перевірку всіх вузлів та компонентів комп'ютера, кожний з яких відмічається контрольними точками або POST-кодами [30].
НВ-1 Автентифікація вузла. Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію.	Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ; КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму; Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.	Реалізовано. Операційна система Windows має можливість оновлення самої себе за допомогою ідентифікації офіційного сервера Mircrosoft з якого виконує завантаження оновлення або це можливо зробити використовуючи VMmanager інсталювавши новий образ.

2.17 Висновки

У другому розділі кваліфікаційної роботи були запропоновані програмні, апаратні та організаційні рішення для забезпечення кращого стану захищеності підприємства, інструкції з їх конфігурування, обрано стандартний функціональний профіль захищеності, описано яким чином реалізовані, або можна реалізувати відповідність його критеріям та розроблено політики безпеки інформації.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Мета економічного розділу

Метою економічного розділу кваліфікаційної роботи є техніко-економічне обґрунтування доцільності запровадження запропонованих в роботі рішень відповідно до засобів забезпечення конфіденційності інформації при використанні віддалених робочих місць на підприємстві.

Технічко-економічні розрахунки повинні містити: орієнтований розрахунок одноразових (капітальних) витрат, експлуатаційних витрат, оцінку величини збитку, загальний ефект від впровадження системи інформаційної безпеки та визначення і аналіз показників економічної ефективності системи інформаційної безпеки.

3.2 Визначення витрат на розробку політики безпеки інформації

Основою для визначення витрат на розробку політики безпеки є концепція сукупної вартості володіння (Total Cost of Ownership), запропонована Gartner Group. У цій моделі враховуються наступні IT-витрати: фіксовані (капітальні) вкладення і поточні витрати.

3.2.1 Розрахунок (фіксованих) капітальних витрат

Капітальні витрати – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

За методикою Gartner Group до фіксованих (капітальних) варто відносити наступні витрати:

– вартість розробки проекту інформаційної безпеки;

– витрати на залучення зовнішніх консультантів;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– вартість створення основного й додаткового програмного забезпечення (ПЗ);

– витрати на первісні закупівлі апаратного забезпечення;

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Техніко-економічні розрахунки на політику безпеки інформації мають містити два показники:

- визначення трудомісткості розробки політики безпеки інформації;
- розрахунок витрат на розробку політики безпеки інформації.

Розрахунок вартості розробки політики безпеки здійснюється з використанням двох показників – трудомісткості розробки ПБ і витрат на її розробку.

Визначення трудомісткості політики безпеки інформації відбувається за формулою (3.1):

$$t = t_{\text{тз}} + t_{\text{в}} + t_{\text{а}} + t_{\text{вз}} + t_{\text{озб}} + t_{\text{овр}} + t_{\text{д}}, \text{годин}, \quad (3.1)$$

де $t_{\text{тз}}$ - тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{\text{в}}$ - тривалість розробки концепції безпеки інформації у організації;

$t_{\text{а}}$ – тривалість процесу аналізу ризиків;

$t_{\text{вз}}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{\text{озб}}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{\text{овр}}$ – тривалість організації виконання відновлювальних робіт забезпечення неперервного функціонування організації;

$t_{\text{д}}$ – тривалість документального оформлення політики безпеки.

Необхідний на розробку політики безпеки інформації час наведено у таблиці 3.1.

Таблиця 3.1 – Часові показники трудомісткості розробки ПБ

Позначення	$t_{тз}$	$t_в$	$t_а$	$t_{вз}$	$t_{озб}$	$t_{овр}$	$t_д$
Кількість часу, год	11	19	18	13	15	14	17

Враховуючи формулу (3.1) трудомісткість розробки ПБ становить:

$$t = 11 + 19 + 18 + 13 + 15 + 14 + 17 = 107 \text{ год.}$$

Тепер необхідно розрахувати витрати на розробку політики безпеки інформації ($К_{рп}$), які складаються з витрат на заробітку плату спеціаліста з інформаційної безпеки ($З_{зп}$) і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації ($З_{мч}$) за формулою:

$$K_{рп} = З_{зп} + З_{мч}, \text{грн.} \quad (3.2)$$

Заробітна плата спеціаліста з ІБ визначається за формулою:

$$З_{зп} = t * З_{іб}, \text{грн,} \quad (3.3)$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями становить – 135 грн/год.

Враховуючи формулу (3.3), витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 107 * 135 = 14445 \text{ грн.}$$

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t * C_{мч}, \text{грн,} \quad (3.4)$$

де t – трудомісткість розробки політики безпеки інформації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р * t_{нал} * С_е + \frac{Ф_{зал} * Н_а}{F_p} + \frac{К_{лпз} * Н_{апз}}{F_p}, грн, \quad (3.5)$$

де Р – встановлена потужність ПК, кВт;

$t_{нал}$ – кількість машин на яких розроблюється політика безпеки;

$С_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920).

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

Річна норма амортизації на ПК визначається за формулою:

$$Н_а = \frac{П_{впк} - Л_{впк}}{П_{впк} * t_{кд}}, грн., \quad (3.6)$$

де $П_{впк}$ – первісна вартість ПК, грн;

$Л_{впк}$ – ліквідаційна вартість ПК, грн;

$t_{кд}$ – час корисної дії, років.

Згідно з формулою (3.5):

$$С_{мч} = 0.22 * 1 * 1.68 + \frac{7500*0.375}{1920} + \frac{4520*0.5}{1920} = 3 \text{ грн.}$$

Згідно з формулою (3.4):

$$З_{мч} = 107 * 3 = 321 \text{ грн.}$$

Згідно з формулою (3.2):

$$К_{рп} = 14445 + 321 = 14766 \text{ грн.}$$

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки обчислюються за формулою:

$$K = К_{рп} + К_{аз} + К_{навч}, \text{грн.}, \quad (3.7)$$

де $К_{навч}$ - витрати на навчання технічних фахівців і обслуговуючого персоналу, тис., грн.;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн.

Витрати на навчання технічних фахівців становлять 1000 грн., які додатково виплачуються спеціалісту ІБ, який розробив політику безпеки.

Витрати на закупівлі апаратного забезпечення та допоміжних матеріалів становлять:

- кількість співробітників, яким необхідно закупити апаратне забезпечення та допоміжні матеріали складає 8 чоловік;
- вартість одного клієнта становить 8000 грн;
- вартість одного монітора становить 3800 грн;
- вартість одного маршрутизатора складає 529 грн.

З цього слідує:

$$К_{аз} = (8000 + 3800 + 529) * 8 = 98632 \text{ грн.}$$

Згідно з формулою (3.7):

$$К = 14766 + 98632 + 1000 = 114398 \text{ грн.}$$

3.2.2 Розрахунок експлуатаційних (поточних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

За методикою Gartner Group до поточних (експлуатаційних) варто відносити наступні витрати:

- вартість Upgrade-відновлення й модернізації системи ($С_в$);

- витрати на керування системою в цілому ($С_к$);

- витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ – "активність користувача").

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки розраховуються за формулою:

$$С = С_в + С_к + С_{ак}, тис. грн. \quad (3.8)$$

$С_в$ = 0 грн. – цим буде займатися системний адміністратор підприємства.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{єв} + С_е + С_{ел} + С_о + С_{тос}, грн. \quad (3.9)$$

$С_н$ – витрати на навчання адміністративного персоналу й кінцевих користувачів;

$С_а$ - річний фонд амортизаційних відрахувань;

$С_з$ - річний фонд заробітної плати інженерно-технічного персоналу;

$С_{єв}$ – єдиний внесок на загальнообов’язкове державне соціальне страхування;

$С_е$ - вартість електроенергії;

$С_о$ - витрати на залучення сторонніх організацій для виконання деяких видів обслуговування;

$С_{тос}$ – витрати на технічне і адміністративне адміністрування та сервіс.

Річний фонд заробітної плати інженерно-технічного персоналу ($С_з$) розраховується за формулою:

$$С_з = З_{осн} + З_{дод}, грн., \quad (3.10)$$

де $З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік.

Вартість електроенергії, що споживається апаратурою системою ІБ протягом року ($С_е$) у конкретному випадку становить 0 грн. так як немає потреби додатковому устаткуванні.

Обов'язки інженерно технічного персоналу будуть покладені на працівника підприємства, тому йому буде нарахована додаткова заробітна плата, що складає 8% від його основної заробітної плати - 20000 грн.

У зв'язку із тим, що обов'язки інженерно-технічного персоналу будуть покладені на адміністратора безпеки, йому буде нарахована додаткова заробітна плата у вигляді 8% від основної. Тому враховуючи формулу (3.9):

$С_з$ = (20000 * 0.08) * 12 = 19200 грн;

$С_н$ = 20 000 грн; - оплата спеціаліста з ІБ за навчання адміністраторів та користувачів (10000 грн. два рази на рік).

$С_{єв}$ = 4224 грн; - єдиного внесок = 22% від річного фонду $С_з$.

$С_{тос}$ = 2556 грн; - вартість ліцензії ПЗ VMmanager на рік.

Згідно з формулою (3.8):

$$С_к = 20\,000 + 19200 + 4224 + 2556 = 45980 \text{ грн.}$$

Витрати викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна орієнтовно визначити, користуючись даними таблиці 3.2 про вагові частки статей витрат у сукупній вартості системи інформаційної безпеки.

Таблиця 3.2 – Вагові частки статей витрат у статті «активність користувача»

Пряма допомога й додаткові настроювання	11%
Неформальне навчання	12%

Розробка додатків	14%
Робота з даними	15%
Формальне навчання	18%
Futz-фактор	30%

Було обрано суму відсотків прямої допомоги й додаткового настроювання та формального навчання.

З цього слідує:

$$C_{ак} = 45980 * 0,29 = 13335 \text{ грн.}$$

Згідно з формулою (3.8):

$$C = 45980 + 13335 = 59315 \text{ грн.}$$

3.3 Оцінка можливого збитку від атаки на вузол або сегмент корпоративної мережі

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

3.3.1 Оцінка величини збитку

Оцінка величини збитку від інформаційної атаки на вузол або сегмент корпоративної мережі буде розрахована для наступних загроз:

- Викрадення, знищення або модифікація ІзОД системний адміністратором;
- Знищення ІзОД через збій у роботі засобів обробки інформації, на яких вона зберігається;
- Пошкодження ІзОД або унеможливлення доступу до неї через використання неякісного ПЗ.

Універсальних рецептів визначення можливого збитку від інформаційної атаки на вузол або сегмент корпоративної мережі не існує. У самому загальному виді передумова розрахунку потенційного збитку полягає в тому, що витрати на забезпечення інформаційної безпеки не повинні перевищувати вартість об'єкта, що захищається, або величину збитку, що може виникнути внаслідок атаки на об’єкт, що захищається.

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих вузлів або сегментів корпоративної мережі;

N – середнє число атак на рік.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V \text{ грн.}, \quad (3.11)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн.;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн.;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum З_с}{F} * t_п, \text{ грн.}, \quad (3.12)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні 176 год.)

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць;

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин.

Вартість відновлення працездатності вузла або сегмента корпоративної мережі розраховується за формулою:

$$П_в = П_{ви} + П_{пв} + П_{зч} \text{ грн.}, \quad (3.13)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховується виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с}{F} * t_{ви}, \text{грн.}, \quad (3.14)$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о}{F} * t_в, \text{грн.}, \quad (3.15)$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{О}{F_r} * (t_п + t_в + t_{ви}), \quad (3.16)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч.

Для першої загрози відповідно до списку загроз наведеного на початку пункту 3.3.1 – рахується розмір втраченого прибутку від реалізації цієї загрози.

Ґрунтуючись на експертному висновку бухгалтера підприємства, втрачений прибуток складає 500000 грн.

Розрахунок ймовірних збитків для другої загрози відповідно до списку загроз наведеного на початку пункту 3.3.1.

Згідно з формулою (3.12):

$$П_{п} = \frac{(17000 * 8)}{176} * 8 \ = 6182 \text{ грн.}$$

Згідно з формулою (3.14):

$$П_{ви} = \frac{(20000 * 2)}{176} * 4 = 909 \text{ грн.}$$

Згідно з формулою (3.15):

$$П_{пв} = \frac{(20000 * 2)}{176} * 2 = 455 \text{ грн.}$$

$П_{зч}$ = 9272 грн. – 8 жорстких дисків вартістю 1159 грн.

Згідно з формулою (3.13):

$$П_{в} = 909 + 455 + 9272 = 10636 \text{ грн.}$$

Згідно з формулою (3.16):

$$V = \frac{7000000 * 12}{2080} * (8 + 4 + 2) = 565385 \text{ грн.}$$

Згідно з формулою (3.11):

$$U = 6182 + 10636 + 565385 = 582203 \text{ грн.}$$

Розрахунок ймовірних збитків для третьої загрози відповідно до списку загроз наведеного на початку пункту 3.3.1.

Згідно з формулою (3.12):

$$П_{п} = \frac{(17000 * 8)}{176} * 8 = 6182 \text{ грн.}$$

Враховуючи формулу (3.14):

$П_{ви}$ = 0 грн. - немає потреби повторного введення інформації.

Враховуючи формулу (3.15):

$П_{пв}$ = 0 грн. - немає потреби повторного введення інформації.

$П_{зч}$ = 0 грн. – немає потреби в заміні устаткування або запасних частин.

Враховуючи формулу (3.13):

$$П_{в} = 0 \text{ грн.}$$

Згідно з формулою (3.16):

$$V = \frac{7000000 * 12}{2080} * 8 = 323077 \text{ грн.}$$

Згідно з формулою (3.11):

$$U = 6182 + 323077 = 329259 \text{ грн.}$$

Таким чином, таким чином загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B = \Sigma_i \Sigma_n * U, \text{ грн.} \quad (3.17)$$

I = 1; - для першої загрози.

I = 2; - для другої та третьої загроз.

N = 1;

Згідно з формулою (3.17) для першої загрози:

$$B = 1 * 1 * 500000 = 500000 \text{ грн.}$$

Згідно з формулою (3.17) для другої загрози:

$$B = 1 * 2 * 582203 = 1164406 \text{ грн.}$$

Згідно з формулою (3.17) для третьої загрози:

$$B = 1 * 2 * 329259 = 658518 \text{ грн.}$$

3.3.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B * R - C \quad (3.18)$$

де В – загальний збиток від атаки на вузол корпоративної мережі, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

С – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

Враховуючи формулу (3.18) для першої загрози:

$$B_1 = 500000 * 0.103 = 51500 \text{ грн.}$$

Враховуючи формулу (3.18) для другої загрози:

$$B_2 = 1164406 * 0.086 = 100139 \text{ грн.}$$

Враховуючи формулу (3.18) для третьої загрози:

$$B_3 = 658518 * 0.086 = 56633 \text{ грн.}$$

Загальна величина збитку складає:

$$B = 51500 + 100139 + 56633 = 208272 \text{ грн.}$$

Враховуючи формулу (3.18):

$$E = 208272 - 59315 = 148957 \text{ грн.}$$

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині кваліфікаційного проекту, здійснюється на основі визначення та аналізу наступних показників:

– сукупна вартість володіння (ТСО);

– коефіцієнт повернення інвестицій ROSI (Return on Investment for Security);

– термін окупності капітальних інвестицій То.

Показник сукупної вартості володіння (ТСО) використовується, якщо величину відверненого збитку від атаки на вузол або сегмент корпоративної мережі важко або неможливо визначити у вартісній формі. У зв'язку з цим такий показник надалі не використовується.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K}, \text{частки одиниці,} \qquad (3.19)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Згідно з формулою (3.19):

$$ROSI = 148957 / 114398 = 1.3$$

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти розрахункове значення ROSI з бажаним значенням показника ефективності $E_н$.

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів, тому в якості $E_н$ варто приймати бажану норму прибутковості альтернативних варіантів вкладення коштів К (на депозитний рахунок у банку).

Проект визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$ROSI > \frac{(N\text{деп} - N\text{інф})}{100} \quad (3.20)$$

де $N_{деп}$ – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, %;

$N_{інф}$ – річний рівень інфляції, %.

Згідно з формулою (3.20):

$$1.3 > \frac{(12 - 10)}{100}$$

Оскільки 1.3 > 0.02, проект є економічно доцільним.

Термін окупності капітальних інвестицій $T_о$ показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_о = \frac{E}{K} = \frac{1}{ROSI}, \text{років.} \quad (3.21)$$

Згідно з формулою (3.21):

$$T_о = \frac{E}{K} = \frac{1}{1.3} = 0{,}76 \text{ років}$$

3.5 Висновки

В цьому розділі було обґрунтовано доцільність запровадження запропонованих в проекті рішень для забезпечення конфіденційності інформації при використанні віддалених робочих місць підприємством, проведені розрахунки витрат на розробку політики безпеки, розраховані капітальні та експлуатаційні витрати, оцінені величини збитку від інформаційної атаки на ІТС підприємства та розраховано загальний ефект від впровадження запропонованої системи інформаційної безпеки. Результати розрахунків:

- капітальні витрати складають 114398 грн;
- експлуатаційні витрати складають 45980 грн;
- величина збитку складає 208272 грн;
- загальний ефект від провадження системи захисту складає 148957 грн;
- коефіцієнт ROSI складає 1.3;
- термін окупності загальних витрат близько 9-ти місяців.

ВИСНОВКИ

У першому розділі було розглянуто чимало загроз для підприємства у випадку віддаленого режиму роботи співробітника. Завдяки цьому, було складено краще розуміння про загрози для конфіденційності інформації підприємства, розглянуто його інформаційні потоки та розроблені моделі порушника та загроз.

У наступному розділі було розглянуто багато можливих рішень для протистояння загрозам, що були розглянуті раніше, запропоновано програмні, апаратні та організаційні рішення для забезпечення кращого стану захищеності підприємства. Розроблено інструкції з конфігурування програмного забезпечення, представлені приклади того, яким чином можна ознайомити працівників з політиками безпеки у форматі курсів та перевірити їх знання у цій сфері у форматі тестів. Також обрано стандартний функціональний профіль захищеності, описано яким чином можна реалізувати відповідність його критеріям та розроблено політики безпеки інформації.

В третьому розділі було розраховано вартість витрат для впровадження запропонованих рішень для визначення доцільності їх впровадження для захисту підприємства від збитків у разі реалізації загроз злочинцями. Було визначено вартість розробки політики безпеки, капітальних та експлуатаційних витрат, оцінені величини збитку від інформаційної атаки на ІТС підприємства та розраховано загальний ефект від впровадження запропонованої системи інформаційної безпеки.

ПЕРЛІК ПОСИЛАНЬ

1. Бизнес на расстоянии: как защитить инфраструктуру [Електронний ресурс] // ptsecurity.com. – 2020. – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/knowledge-base/biznes-na-rasstoyanii-kak-zashchitit-infrastrukturu/.

2. Уязвимости корпоративных информационных систем [Електронний ресурс] // ptsecurity.com. – 2019. – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/#id7.

3. Козлов Р. Безопасный удалённый доступ: как защитить инфраструктуру от злодеев и нерадивых сотрудников [Електронний ресурс] / Роман Козлов // ispsystem.ru. – 2020. – Режим доступу до ресурсу: https://www.ispsystem.ru/news/secure-remote-access-exp.

4. Федосеенко В. Краткая история виртуализации [Електронний ресурс] / Виктория Федосеенко // ispsystem.ru. – 2019. – Режим доступу до ресурсу: https://www.ispsystem.ru/news/brief-history-of-virtualization.

5. Петровский А. Как организовать удалённый рабочий стол с помощью VMmanager [Електронний ресурс] / Алексей Петровский // ispsystem.ru. – 2020. – Режим доступу до ресурсу: https://www.ispsystem.ru/news/vdi-instr.

6. Бездисковая рабочая станция [Електронний ресурс] // wikipedia.org – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Бездисковая_рабочая_станция.

7. Безопасность удаленной работы: проблемы и рекомендации [Електронний ресурс] // tadviser.ru. – 2020. – Режим доступу до ресурсу: https://www.tadviser.ru/index.php/Статья:Безопасность_удаленной_работы:_проблемы_и_рекомендации.

8. Рабочее место сотрудника (в офисе) [Електронний ресурс] // itsave.ru – Режим доступу до ресурсу: http://itsave.ru/бездисковая-рабочая-станция/.

9. Ноутбук [Електронний ресурс] // wikipedia.org – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Ноутбук#Попадание_жидкости.

10. Baker M. Gartner HR Survey Reveals 88% of Organizations Have Encouraged or Required Employees to Work From Home Due to Coronavirus [Електронний ресурс] / Mary Baker // gartner.com. – 2020. – Режим доступу до ресурсу: https://www.gartner.com/en/newsroom/press-releases/2020-03-19-gartner-hr-survey-reveals-88--of-organizations-have-e.

11. VDI: как работает, плюсы, минусы и кому подходит [Електронний ресурс] // selectel.ru. – 2020. – Режим доступу до ресурсу: https://selectel.ru/blog/vdi-technology-review/.

12. Підкачування сторінок [Електронний ресурс] // wikipedia.org – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Підкачування_сторінок.

13. ПОНЯТИЕ ТОНКОГО И ТОЛСТОГО КЛИЕНТА [Електронний ресурс] // testmatick.com. – 2021. – Режим доступу до ресурсу: https://testmatick.com/ru/ponyatie-tonkogo-i-tolstogo-klienta/.

14. Менеджер паролей [Електронний ресурс] // wikipedia.org – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Менеджер_паролей.

15. Касунич К. 9 лучших менеджеров безопасных паролей [Електронний ресурс] / Кэти Касунич // vpnmentor.com. – 2021. – Режим доступу до ресурсу: https://ru.vpnmentor.com/blog/лучшие-менеджеры-безопасные-паролей/.

16. Обзор менеджеров паролей [Електронний ресурс] // habr.com. – 2021. – Режим доступу до ресурсу: https://habr.com/ru/company/cloud4y/blog/581916/.

17. CHOOSE THE PLAN FOR YOU [Електронний ресурс] // dashlane.com – Режим доступу до ресурсу: https://www.dashlane.com/plans.

18. RDP [Електронний ресурс] // itglobal.com – Режим доступу до ресурсу: https://itglobal.com/ru-ru/company/glossary/rdp/.

19. По какому принципу работает TeamViewer? [Електронний ресурс] // faq-teamviewer.ru. – 2018. – Режим доступу до ресурсу: https://faq-teamviewer.ru/faq/po-kakomu-printsipu-rabotaet-teamviewer.

20. VNC [Електронний ресурс] // ispsystem.ru – Режим доступу до ресурсу: https://docs.ispsystem.ru/vmmanager-admin/vnutrennee-ustrojstvo/ispol-zuemye-podsistemy/vnc.

21. Установка Windows Server 2019 [Електронний ресурс] // softcomputers.org – Режим доступу до ресурсу: https://softcomputers.org/blog/ustanovka-windows-server-2019/.

22. Как записать Windows на флешку [Електронний ресурс] // softcomputers.org – Режим доступу до ресурсу: https://softcomputers.org/blog/kak-zapisat-windows-na-flesh/.

23. WinSetupFromUSB 1.10.exe [Електронний ресурс] // winsetupfromusb.com – Режим доступу до ресурсу: http://www.winsetupfromusb.com/files/download-info/winsetupfromusb-1-10-exe.

24. Как загрузиться с флешки из под биоса? Инструкция. [Електронний ресурс] // softcomputers.org – Режим доступу до ресурсу: https://softcomputers.org/blog/kak-zagruzitsya-s-fleshki/.

25. Установка и настройка обновлений Windows 10 [Електронний ресурс] // comss.ru. – 2019. – Режим доступу до ресурсу: https://www.comss.ru/page.php?id=5305.

26. Моск Д. Установка и настройка VMmanager 5 на Linux [Електронний ресурс] / Дмитрий Моск // dmosk.ru. – 2020. – Режим доступу до ресурсу: https://www.dmosk.ru/instruktions.php?object=vmmanager#install.

27. Что такое нода? [Електронний ресурс] // bitte.net.ua – Режим доступу до ресурсу: https://bitte.net.ua/blog/chto-takoe-noda/.

28. Download TightVNC [Електронний ресурс] // tightvnc.com – Режим доступу до ресурсу: https://tightvnc.com/download.php.

29. 237686436.jpg 3 783x2 477 pixels [Електронний ресурс] // rozetka.com.ua – Режим доступу до ресурсу: https://content.rozetka.com.ua/goods/images/original/237686436.jpg.

30. POST [Електронний ресурс] // wikipedia.org – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/POST.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	1	
5	А4	1 Розділ	22	
6	А4	2 Розділ	78	
7	А4	3 Розділ	17	
8	А4	Висновки	1	
9	А4	Список літератури	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу на тему:
Засоби забезпечення конфіденційності інформації при використанні віддалених робочих місць на підприємстві
Мінгальова Владислава Євгеновича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 138 сторінках та містить 61 рисунок, 21 таблицю, 30 джерел та 4 додатка.

Мета роботи: забезпечення конфіденційності інформації при використанні віддалених робочих місць на підприємстві.

У першому розділі був проведений аналіз загроз конфіденційності інформації у віддаленому режимі роботи, складені модель порушника та модель загроз.

У спеціальній частині був проведений аналіз можливих рішень для протистояння загрозам, що були розглянуті у першому розділі, розроблено інструкції з конфігурування програмного забезпечення, обрано стандартний функціональний профіль захищеності, описано яким чином можна реалізувати відповідність його критеріям. Також розроблено політики безпеки інформації та формат ознайомлення співробітників з ними.

В економічній частині обґрунтована економічна доцільності впровадження методики застосування засобів забезпечення конфіденційності інформації при використанні віддалених робочих місць на підприємстві.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник