ЗАТВЕРДЖЕНО
Наказом КЗ «Бахмутський
медичний фаховий коледж»
№ 130-о/д від 30.05.2024 р.

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗАКЛАДУ ОСВІТИ

КОМУНАЛЬНИЙ ЗАКЛАД
«БАХМУТСЬКИЙ МЕДИЧНИЙ ФАХОВИЙ КОЛЕДЖ»

Політика інформаційної безпеки закладу освіти Комунальний заклад «Бахмутський медичний фаховий коледж» базується на рекомендаціях, розроблених в рамках проекту HRS (Health Reform Support) і враховує особливості діяльності підприємства, як надавача освітніх послуг, що належить до сфери охорони здоров'я. Дана політика затверджена керівником навчального закладу, доведена до всіх співробітників КЗ «Бахмутський медичний фаховий коледж» і відповідно виконується, як зазначено. До вказаної політики можливе внесення корегувань, що оформлюються у вигляді доповнень, затверджуються керівником, виходячи з потреб навколишнього та інформаційного середовища, а також при змінах у вимогах регулюючих органів, що опікуються кібербезпекою об'єктів критичної інфраструктури України.

Відомості про організацію функціонування Політики безпеки

№	Назва	Опис
1.	Назва закладу освіти	Комунальний заклад «Бахмутський медичний фаховий коледж»
2.	Керівник	Красножон Наталя Миколаївна
3.	Web-сайт	http://amedu.edu.ua
4.	Електронна пошта	artemovsk_meduchil@ukr.net
5.	Юридична адреса	Україна, 84500, Донецька обл., м. Бахмут, вул. Носакова, 9
6.	Місце фізичного розташування	Україна, Полтавська обл. Полтавський р-н, смт. Нові Санжари, Перемоги, 7
7.	Дата останньої редакції документа	30.05.2024
8.	Дата затвердження документа	30.05.2024
9.	Дата набрання чинності документа	01.06.2024
10.	Внутрішні підрозділи організації	Канцелярія; Бухгалтерія; Навчальна частина; Кадрова служба
11.	Зовнішні організації	Управління (головне управління) охорони здоров`я Донецької обласної державної адміністрації; Міністерство охорони здоров’я України; Міністерство освіти України
12.	Відповідальний за інформаційну безпеку	Самойленков Олексій Євгенович
13.	Постачальники послуг (Internet, центр сертифікації ключів, on-line сервіси)	ДП «Інфоресурс», Google LLC • Інші постачальники відображені у відповідному документі та їх перелік не може бути оприлюднений
14.	Електронний зв'язок	Електронна пошта, Rakuten Viber Messenger

15.	Аудит ідентифікаторів (КЕП)	Раз на рік
16.	Довжина паролів служб та сервісів	Не менше 10 символів
17.	Зміна паролів	Раз на 2 місяці
18.	Антивірусне програмне забезпечення	Avast Free Antivirus
19.	Виробник антивірусного програмного забезпечення	AVAST Software
20.	Оновлення антивірусного програмного забезпечення	Автоматичне оновлення від виробника програмного забезпечення
21.	Безпека фізичного рівня	Персональна відповідальність співробітників (під час дистанційної роботи)
22.	Обладнання	Персональні комп'ютери, пристрої зчитування карт доступу (токен-карти, ідентифікатори для замовлення документів про освіту)
23.	Різне	Освітні послуги, що надає заклад освіти та результати діяльності у сфері освіти відображаються у Єдиній державній електронній базі освіти, надавач послуг Державне підприємство «Інфоресурс», відповідно до Закону України «Про затвердження Положення про Єдину державну електронну базу з питань освіти» від 05 жовтня 2018 р. за № 1132/32584
24.	Контактний номер телефону	+380506319313

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
КОМУНАЛЬНИЙ ЗАКЛАД
«БАХМУТСЬКИЙ МЕДИЧНИЙ ФАХОВИЙ КОЛЕДЖ»

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ДАТА ОСТАНЬОЇ РЕДАКЦІЇ 30 ТРАВНЯ 2024 РОКУ

ДОКУМЕНТ ЗАТВЕРДЖЕНО

КРАСНОЖОН НАТАЛЯ

МИКОЛАЇВНА

Підпис _____

ЗМІСТ

Комунальний заклад «Бахмутський медичний фаховий коледж» Політика інформаційної безпеки	
Назва: ВСТУПНА ЧАСТИНА	п.1.1.-1.5
Дата затвердження 30.05.2024 Дата набрання чинності: 01.06.2024	Огляд: Щорічний Інформаційна безпека закладів освіти; Інформаційна безпека закладів охорони здоров'я

ВСТУПНА ЧАСТИНА

1.1. Загальні положення

Ця політика інформаційної безпеки визначає основні засади забезпечення належного рівня інформаційної безпеки Комунального закладу «Бахмутський медичний фаховий коледж», далі – Політика або скорочено ПІБ. ПІБ служить центральним програмним документом з інформаційної безпеки, з яким повинні бути ознайомлені всі працівники закладу освіти, підрядники (постачальники послуг), споживачі освітніх послуг, і визначає дії, застереження, заборони, яких повинні дотримуватися всі користувачі інформаційних та цифрових активів закладу освіти. Політика роздруковується та затверджується директором коледжу та зберігається у відповідального за інформаційну безпеку. У разі неможливості призначити окремого відповідального за інформаційну безпеку із-за обмеженості людського ресурсу закладу, функцію відповідального за інформаційну безпеку виконує головний бухгалтер закладу.

Належний рівень інформаційної безпеки, це такий стан фізичного, інформаційного середовища та середовища користувачів інформаційних та цифрових активів Комунального закладу «Бахмутський медичний фаховий коледж», який гарантує конфіденційність, доступність, цілісність інформації закладу освіти та спостережність і контрольованість систем/підсистем, в яких ця інформація циркулює.

Належний рівень інформаційної безпеки досягається за рахунок вмілого застосування комплексу програмних/технічних засобів та організаційних заходів, спрямованих на забезпечення захищеності даних від зловмисного

використання.

Вимоги та обмеження ПІБ, застосовуються до мережевої інфраструктури, баз даних, носіїв інформації, засобів шифрування, друкованих документів, мультимедіа файлів, засобів бездротового зв'язку, телекомунікаційних систем, аудіо повідомлень та будь-яких інших засобів, що використовуються для передачі, обробки та зберігання інформації у всіх апаратних, програмних та інших інформаційних та цифрових системах забезпечення освітнього процесу. Цієї політики повинні дотримуватися всі штатні та тимчасові працівники в усіх місцях (на робочому місці чи працюючи віддалено), а також підрядники – постачальники послуг, які працюють з закладом освіти.

1.2. Глосарій

1.2.1. Загальні терміни та абревіатури, які використовуються в цьому документі

Актив – матеріальні та нематеріальні об’єкти або інформація, що мають цінність для закладу освіти.

Аутентифікація – процес визначення належного інформаційній системі користувача з метою надання йому відповідних прав.

Брандмауер – спеціальне обладнання або програмне забезпечення, що працює на комп'ютері, яке дозволяє або відмовляє в проходженні трафіку через нього, на основі набору правил.

ВІБ – відповідальний за інформаційну безпеку, призначена особа, яка відповідає за впровадження та дотримання Політики інформаційної безпеки в закладі освіти.

Вірус – шкідливе програмне забезпечення, здатне відтворювати сама себе і зазвичай здатне завдати великої шкоди файлам або іншим програмам на комп'ютері, який воно атакує.

Виток інформації – випадкове або навмисне поширення конфіденційної інформації в межах діяльності закладу освіти.

Доступність інформації – властивість, яка гарантує те, що забезпечується своєчасний доступ авторизованих осіб та процесів до інформації, а також

відсутні простої в процесі її обробки, тобто коли інформація знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і у той час, коли вона йому необхідна. У випадку втрати інформації існує можливість своєчасного її відновлення.

ЄДЕБО – єдина державна електронна база освіти.

Журналювання – процес фіксації дій користувача інформаційної системи.

ЗО – заклад освіти.

Зовнішні носії інформації – компакт-диски, DVD-диски, дискети, флешки, USB, флеш- накопичувачі та інші.

ІБ - Інформаційна безпека, це процес, який забезпечує збереження визначених Політикою інформаційної безпеки та спрямований на запобігання несанкціонованим діям в інформаційній системі, що включає сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи інформаційної системи.

ІС – Інформаційна система, організаційно-технічна система, у якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

ІТ – Інформаційна технологія.

Керівник– керівник закладу освіти.

КЗ БМФК – Комунальний заклад «Бахмутський медичний фаховий коледж».

КЕП – кваліфікований електронний підпис.

Конфіденційність інформації – властивість, яка гарантує те, що доступ до інформації можуть одержати тільки авторизовані особи або процеси.

Користувач - будь-яка особа зі складу персоналу ЗО, уповноважена на доступ до певного інформаційного ресурсу.

Користувачі з можливостями запиту (лише для читання) – особи, яким на основі прав доступу заборонено додавати, видаляти або змінювати записи в базі даних та інших доступних їм масивах інформації. Їх системний доступ обмежується лише зчитуванням інформації.

Користувачі з можливостями редагування/оновлення – особи, яким дозволено на основі прав доступу додавати, видаляти або змінювати записи в базах даних та інших масивах інформації, що супроводжують діяльність закладу освіти.

Локальна мережа – комп'ютерна мережа в межах приміщення закладу освіти.

ПІБ – Політика інформаційної безпеки, це центральний, програмний документ, який визначає основні засади забезпечення належного рівня інформаційної безпеки закладу освіти.

Персонал – всі працівники ЗО, які використовують інформаційні ресурси закладу, комп'ютерне, телекомунікаційне і офісне обладнання відповідно до своїх посадових обов’язків.

ПК – персональний комп’ютер.

Привілейовані користувачі – системні адміністратори та інші особи, які конкретно ідентифіковані та мають санкціонований керівництвом доступ до певних баз даних та масивів інформації (ЄДЕБО, фінансові бази даних, бази даних господарської діяльності).

Провайдер – надавач послуг користуванням мережею Internet.

РГІБ – робоча група з інформаційної безпеки, колективний керівний орган системи управління інформаційною безпекою ЗО.

Спостережність системи – властивість, що дозволяє фіксувати діяльність користувачів і процесів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки або забезпечення відповідальності за певні дії.

СУІБ – Система управління інформаційною безпекою, це комплекс організаційних, програмних, технічних і фізичних заходів, спрямованих на управління ризиками, що пов'язані з використанням у ЗО інформації та інформаційних технологій.

Третя сторона – фізична чи юридична особа, яка перебуває у будь-яких договірних відносинах з ЗО та є стороною таких відносин.

Цілісність інформації – властивість, яка гарантує те, що інформація не містить помилок, є актуальною, вичерпною, будь-які зміни інформації здійснюються авторизованими особами чи процесами.

Шифрування – процес перетворення інформації, використовуючи алгоритм, щоб зробити її нечитабельною для будь-кого, крім тих, хто має авторизовану «потребу знати».

VLAN – Віртуальна локальна мережа – локальна мережа, яка використовується для сегментації мережевого трафіку з метою адміністрування та безпеки.

VPN – Віртуальна приватна мережа – забезпечує безпечну передачу даних та доступ через загальнодоступні мережі.

1.2.2. Інші терміни, що вживаються у цій Політиці, застосовуються в значеннях, визначених чинним законодавством України.

1.3. Застосовані положення

Нижче наведено перелік нормативних та регулюючих законів, актів, стандартів на основі яких розроблено ПІБ КЗ БМФК.

- Закон України «Про основні засади забезпечення кібербезпеки України»;
- Закон України «Про інформацію»;
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Закон України «Про електронні документи та електронний документообіг»;
- Закон України «Про освіту»;
- Закону України «Про затвердження Положення про Єдину державну електронну базу з питань освіти»;
- Постанова КМУ №518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»;
- ISO/IEC27000:2019 - Інформаційні технології - Методи і засоби

забезпечення безпеки - Системи управління інформаційною безпекою - Загальні відомості і словник;

- ISO/IEC 27001:2013 - Інформаційні технології - Методи захисту - Системи управління інформаційною безпекою – Вимоги;
- ISO/IEC 27002:2013/COR 2:2015 - Інформаційні технології - Методи захисту - Звід рекомендованих правил для управління інформаційною безпекою;
- ISO/IEC 27003:2017 - Інформаційні технології - Методи безпеки - Системи управління інформаційною безпекою – Керівництво;
- ISO/IEC 27004:2016 - Інформаційні технології - Методи безпеки - Управління інформаційною безпекою - Моніторинг, вимір, аналіз і оцінка;
- ISO/IEC 27005:2018 - Інформаційні технології - Методи безпеки - Управління ризиками інформаційної безпеки;
- ISO/IEC 15408-1:2009 - Загальні критерії оцінки захищеності інформаційних технологій;
- ISO/IEC TS 27008:2019 - Методи безпеки - Вказівки для оцінки засобів контролю інформаційної безпеки;
- ISO 27032 – Інформаційні технології. Методи захисту;
- ISO 27035 – Управління інцидентами.

1.4. Відповідальна особа за інформаційну безпеку

Відповідальний за інформаційну безпеку Комунального закладу «Бахмутський медичний фаховий коледж» - призначена особа зі складу персоналу закладу, який (яка) відповідає за дотримання належного рівня інформаційної безпеки закладу освіти, контролює всю поточну діяльність, пов'язану з розробкою, впровадженням та підтримкою політики інформаційної безпеки закладу, зберігає актуальний затверджений примірник ПІБ у себе на робочому місці та при необхідності надає до нього доступ. Чинним ВІБ є: Самойленков Олексій, ukrmen@gmail.com, +380506319313.

1.5. Робоча група з інформаційної безпеки

Робоча група з інформаційної безпеки закладу освіти, це колективний керівний орган з управління системою інформаційної безпеки Комунального закладу «Бахмутський медичний фаховий коледж».

Всі члени робочої групи з інформаційної безпеки (РГІБ), визначені в рамках цієї політики, призначаються директором, відповідним наказом. Термін повноважень членів РГІБ складає один рік та може бути продовжений відповідним рішенням директора. Чинними членами РГІБ є:

- Воронцова Олеся – начальник кадрової служби;
- Завражна Ганна -адміністратор ЄДЕБО;
- Кірпа Юлія – головний бухгалтер.

РГІБ збирається щоквартально, або частіше за потреби, щоб обговорити питання інформаційної безпеки та розглянути проблеми, які виникли протягом кварталу. РГІБ визначає та затверджує програму щорічного навчання персоналу з інформаційної безпеки, та переглядає/оновлює політику інформаційної безпеки, якщо це необхідно.

РГІБ вирішує нагальні питання інформаційної безпеки в міру їх виникнення, а також приймає та схвалює необхідні заходи безпеки, які повинні бути вжиті. Відповідальність РГІБ полягає в тому, щоб визначити ризики інформаційної безпеки та вчасно вжити необхідних заходів з мінімізації чи усунення.

РГІБ контролює ведення журналу подій інформаційної безпеки. Ведення цього журналу здійснюється на постійній основі. До журналу вносяться дата події, дії, вжиті для вирішення події, а також рекомендації щодо подальших дій персоналу, якщо це доречно. Цей журнал розглядається РГІБ під час щоквартальних засідань.

Відповідальний за ІБ забезпечує ведення журналу подій інформаційної безпеки, а також напрацьовує на його основі та подає на розгляд РГІБ пропозиції з підвищення рівня ІБ, покращення захисту інформації та активів Комунального закладу «Бахмутський медичний фаховий коледж».

Комунальний заклад «Бахмутський медичний фаховий коледж» Політика інформаційної безпеки	
Назва: ОБОВ'ЯЗКИ СПІВРОБІТНИКІВ	п.2.1.-2.9
Дата затвердження 30.05.2024 Дата набрання чинності: 01.06.2024	Огляд: Щорічний Інформаційна безпека закладів освіти; Інформаційна безпека закладів охорони здоров’я

2. ОБОВ'ЯЗКИ СПІВРОБІТНИКІВ

2.1. Вимоги до співробітників

Першою лінією захисту в системі управління інформаційною безпекою Комунального закладу «Бахмутський медичний фаховий коледж» є співробітники або користувачі. Користувачі несуть відповідальність за безпеку всіх даних, які можуть надходити до них у будь-якому форматі.

Для ідентифікації персоналу під час фізичного перебування в будівлі закладу освіти – використовуються ідентифікуючі беджі, які співробітники коледжу повинні носити на собі та які легко переглядати іншім. Це допомагає підтримувати фізичну безпеку та активів закладу освіти. Підрядникам, представники третьої сторони, які також можуть знаходитися в будівлі ЗО (або приміщенні, що використовується для забезпечення роботи ЗО), у разі необхідності надаються беджі іншого зразка. Здобувачі освіти та абітурієнти (під час вступної компанії) не повинні мати беджів, але не можуть знаходитися у службових приміщеннях та приміщеннях з обмеженим доступом.

Обов'язком всіх працівників закладу є вжиття необхідних заходів для забезпечення фізичної безпеки активів Комунального закладу «Бахмутський медичний фаховий коледж». Якщо будь хто з співробітників бачить невстановлену особу в службовому приміщені чи приміщені з обмеженим доступом, він/вона повинен вжити всіх можливих заходів для виведення такої особи із зазначеного приміщення та проінформувати про такий випадок ВІБ або директора закладу освіти. Усі відвідувачі приміщення, де здійснюється робота

закладу повинні заходити через стійку реєстрації та знаходитись тільки в тих приміщеннях, які дозволені для перебування відвідувачів. У разі спільного використання приміщень з іншим закладом (організацією) – норма зберігається. Захист робочих станцій. Всі робочі станції (ПК), які знаходяться в закладі не повинні залишати ЗО без відповідного дозволу керівника чи ВІБ. Всім новим користувачам надається первинний інструктаж на робочому місці щодо правил використання та зберігання робочих станцій закладу. У разі запровадження дистанційної роботи переміщення робочих станцій здійснюється лише після відповідного розпорядження директора закладу освіти.

Робочі станції, що використовуються для забезпечення діяльності Комунального закладу «Бахмутський медичний фаховий коледж», можуть містити конференційні данні особового, кадрового чи фінансового характеру, тому слід дотримуватися максимальної обережності, щоб ці дані не були скомпрометовані. При використані робочих станцій за межами закладу освіти (під час дистанційної або віддаленої роботи) користувач повинен вжити всіх можливих заходів із забезпечення безпечного зберігання та використання ПК, інформації та програмного забезпечення, що на ньому знаходяться.

На робочих станціях дозволено використання тільки ліцензійного програмного забезпечення та/або спеціального програмного забезпечення, яке надається авторизованим виробником разом з апаратним забезпеченням.

ПК без нагляду. Робочі станції, які залишаються без нагляду повинні бути заблоковані користувачем при виході з робочої зони (робочого місця). Це правило нагадується усьому персоналу під час навчань з інформаційної безпеки. Також на робочих станціях повинно застосовуватись налаштування автоматичного блокування екрана після десяти хвилин бездіяльності. Персоналу заборонено відключати чи змінювати це налаштування без відповідного дозволу ВІБ.

У разі використання власних робочих станцій у зв’язку з виробничими потребами або під час дистанційної роботи – співробітники коледжу повинні вжити всіх заходів з метою забезпечення збереження інформації та недопущення

її витоку.

Домашнє використання ПК. Дозволяється використовувати лише обладнання (комп’ютери, ноутбуки, смартфони), які мають ліцензійне програмне забезпечення та засоби антивірусного захисту. З метою збереження конфіденційності та цілісності даних, що обробляться власними пристроями, з персоналом, що має на це дозвіл, проводитись інструктаж ВІБ. З метою обробки даних, що супроводжують діяльність Комунального закладу «Бахмутський медичний фаховий коледж», дозволено використовувати лише програмне забезпечення, що схвалено відповідним документом (переліком погодженого програмного забезпечення або ПІБ).

Персональні комп'ютери, що надаються для дистанційної роботи, повинні використовуватися виключно в службових цілях. Співробітники закладу освіти повинні бути ознайомлені і розуміти перелік заборонених видів діяльності, який викладений у п.2.2. нижче. Самовільне переналаштування або зміни конфігурації не допускаються на комп'ютерах, що використовуються для дистанційної роботи персоналом.

Збереження права власності. Усі програмні засоби та документація, що встановлюється на робочих станціях або надаються співробітникам для забезпечення діяльності ЗО, є власністю закладу, якщо це не передбачено іншим договором. Виключенням можуть бути випадки використання на робочих станціях програмного забезпечення придбаного за власний кошт працівником коледжу.

2.2. Заборонена діяльність

Співробітникам Комунального закладу «Бахмутський медичний фаховий коледж» забороняється здійснювати дії, описані в пункті 2.2 цієї ПІБ. Перелік не є вичерпним. На інші заборонені види діяльності є посилання в інших місцях цього документа.

- Дії що призводять до збою інформаційної системи. Навмисні дії що призводять до збою інформаційної системи категорично заборонені.

Користувачі можуть не усвідомлювати, що вони спричинили збій системи, але якщо буде виявлено, що збій стався в результаті дії користувача, повторні дії користувача, що призводять до збою інформаційної системи можуть розглядатися як навмисний вчинок.

- Спроба несанкціонованого доступу до інформаційного ресурсу або спроба обійти функцію безпеки. Це включає в себе запуск програм для злому паролів або програм для сканування локальної мережі з метою виявлення вразливостей, а також спроби обійти заборону на доступ до інформаційних ресурсів.
- Завантаження або спроба завантаження комп'ютерних вірусів, троянів, шпигунських програм або інших видів шкідливого програмного забезпечення в інформаційну систему. Винятком може бути перевірка стійкості системи уповноваженим персоналом або представниками третьої сторони, що авторизовано перевіряє СУІБ.
- Несанкціонований перегляд інформації. Умисний, несанкціонований доступ або перегляд інформації, до якої не надавалися права на доступ чи перегляд відповідно до правила «надання мінімально необхідного доступу» для виконання службових завдань. Цілеспрямована спроба перегляду або доступу до інформації, до якої не було надано доступу за визначеною в ПІБ процедурою, суворо заборонено.
- Використання особистого або недозволеного програмного забезпечення на робочих станціях. Використання особистого або недозволеного програмного забезпечення на робочих станціях закладу освіти заборонено. Все програмне забезпечення, встановлене на робочих станціях, має бути затверджене та дозволене до використання. Винятком можуть бути власні комп’ютери, що використовуються в умовах дистанційної або віддаленої роботи. В цьому випадку передбачено надання доступу виключно до програмного забезпечення, що представлені у вигляді on-line сервісів і не передбачає встановлення окремого додатка на такий комп’ютер.
- Використання неліцензійного програмного забезпечення. Все програмне

забезпечення, яке встановлене на робочих станціях повинно бути ліцензійним та/або дозволеним до використання.

- Використовувати дозволене програмне забезпечення не належним чином. Порушувати або намагатися порушити умови використання або ліцензійну угоду будь-якого програмного продукту, що дозволено до використання на робочих станціях, суворо заборонено.
- Використовувати інформаційні системи не належним чином. Брати участь у будь-якій діяльності з будь-якою метою, яка є незаконною або суперечить чинній політиці інформаційної безпеки, суворо заборонено.

2.3. Користування мережею Internet та електронною поштою

Електронні засоби комунікації та Internet є дієвими інструментами підвищення продуктивності. Ділове використання електронних комунікацій заохочується. Однак усі системи електронного зв'язку та всі повідомлення, що генеруються на обладнанні, що належить Комунальному закладу «Бахмутський медичний фаховий коледж», або обробляються на пристроях, що належать закладу, вважаються власністю Комунального закладу «Бахмутський медичний фаховий коледж», а не власністю окремих користувачів. Також до зазначеного переліку відносяться данні та інформаційні повідомлення, що обробляються співробітниками на власних пристроях під час дистанційної або віддаленої роботи. Отже, ця політика поширюється на всіх співробітників і підрядників (третю сторону) та охоплює всі електронні комунікації, включаючи, але не обмежуючись ними, телефони, електронну пошту, голосову пошту, обмін миттєвими повідомленнями, Internet, персональні комп'ютери та сервери.

Надані співробітникам інформаційні ресурси, такі як робочі станції або ноутбуки, комп'ютерні системи, мережі, електронна пошта, програмне забезпечення, а також доступ до Internet, призначені для використання в цілях забезпечення діяльності закладу освіти. Однак особисте використання допустимо до тих пір, поки це:

- не відволікає від виконання роботи або функціональних обов’язків;

- не зменшує продуктивність від час виконання службових обов’язків та завдань;
- не перешкоджає діяльності закладу освіти;
- не веде до наступного:

1) незаконна діяльність – використання інформаційних ресурсів Комунального закладу «Бахмутський медичний фаховий коледж» для досягання незаконних цілей або для здійснення правопорушень, суворо заборонено;
2) порушення авторських прав – це включає скачування, тиражування та використання піратського програмного забезпечення, музики, книг, відео та аудіо файлів, а також незаконне дублювання та/або розповсюдження інформації та іншої інтелектуальної власності, яка перебуває під авторським правом;
3) комерційне використання – використання інформаційних ресурсів Комунального закладу «Бахмутський медичний фаховий коледж» для отримання особистої вигоди суворо заборонено;
4) політична діяльність – вся політична діяльність суворо заборонена в приміщеннях та з використанням інформаційних ресурсів Комунального закладу «Бахмутський медичний фаховий коледж». Заклад заохочує своїх співробітників голосувати та активно брати участь у виборчому процесі, але ці заходи не повинні виконуватися з використанням активів та ресурсів закладу освіти і впливати на робочий процес коледжу;
5) переслідування та дискримінація – забороняється використання комп'ютерів, електронної пошти, обміну миттєвими повідомленнями, текстових повідомлень та Internet способами, які є образливими для інших або шкідливими та аморальними. Наприклад, показ або передача зображень, повідомлень і відео сексуального характеру суворо заборонені. Інші приклади неправильного використання включають, але не обмежуються ними, етнічні образи, расові коментарі, або все, що може бути розтлумачено як переслідування, дискримінація, зневажливе

ставлення, вираз погроз або прояв неповаги до інших;

6) Небажана електронна пошта та повідомлення - усі повідомлення зроблені з використанням ІТ-ресурсів Комунального закладу «Бахмутський медичний фаховий коледж» повинні бути адресними та доцільними. Розповсюдження «небажаної» пошти, наприклад, листів щастя, реклами або несанкціонованих клопотань, забороняється. Якщо користувачі отримали будь-яке з перерахованого вище повідомлень, необхідно їх видалити та нікому не пересилати.

Заклад зберігає за собою право здійснювати моніторинг змісту будь-якого електронного повідомлення та комунікації, що генерується або передається з використанням інформаційних активів Комунального закладу «Бахмутський медичний фаховий коледж», або особистого обладнання працівників під час дистанційної та віддаленої роботи, але лише тієї інформації, що стосується діяльності закладу освіти. Це робиться з метою належного обслуговування та захисту інформаційно- телекомунікаційного обладнання, мереж та ефективного використання наявних ресурсів. Моніторинг може здійснюватися постійно або час від часу. Для цього можуть застосовуватися різні методи моніторингу. Наприклад, перевірка історії браузера, перегляд журналювання операційної системи та ін. Інші приклади, коли електронні комунікації можуть контролюватися, включають, але не обмежуються, дослідженнями та тестуваннями спрямованими на оптимізацію ІТ-ресурсів, усунення технічних проблем та виявлення закономірностей зловживань або незаконної діяльності.

Заклад освіти залишає за собою право на власний розсуд переглядати робочі файли або службові електронні повідомлення будь-якого співробітника в обсязі, необхідному для забезпечення ефективного використання всіх службових електронних носіїв і засобів комунікації відповідно до всіх чинних законів і нормативних актів, а також цієї Політики інформаційної безпеки.

2.4. Доступ до Internet та сервісів глобальної мережі

В межах приміщень, де здійснює свою діяльність Комунальний заклад «Бахмутський медичний фаховий коледж», доступ в Internet надається тільки тим співробітникам, хто його потребує для виконання службових обов'язків. Доступ до Internet це ресурс, за який Комунальний заклад «Бахмутський медичний фаховий коледж» витрачає кошти тому його використання потребує виконання наступних вимог. Персонал, що має доступ до Internet, не повинен використовувати цей доступ для розваг, прослуховування музики чи радіо, прослуховування онлайн аудіо книг та перегляду фільмів та інших медійних файлів тощо. Забороняється використовувати доступ до Internet для особистої комерційної діяльності чи вирішення своїх побутових питань. Треба розуміти, що використання цього ресурсу не цільовим шляхом створює додаткові загрози інформаційної безпеки.

Персонал повинен розуміти, що індивідуальне використання Internet в межах приміщень коледжу, контролюється, і якщо виявиться, що співробітник витрачає надмірну кількість часу, витрачає великі обсяги трафіку для особистого чи нецільового користування, або відвідує ресурси, які небезпечні з точки зору забезпечення інформаційної безпеки, то до нього/неї будуть вжиті дисциплінарні заходи.

Ресурси які заборонено відвідувати, такі як ігрові інтернет-сайти, торенти, файлообмінники, порносайти, чати та онлайн програми для обміну музикою, тощо, автоматично блокуються за допомогою відповідних налаштувань в телекомунікаційному обладнанні, що використовується в приміщенні закладу освіти. Перелік заборонених ресурсів постійно контролюється і оновлюється в міру необхідності. Будь-який співробітник, який цілеспрямовано, неодноразово буде намагатися відвідати заборонені ресурси в Internet через локальну мережу коледжу, буде притягнутий до дисциплінарної відповідальності і може бути звільнений.

В закладі освіти здійснюються спеціальні запобіжні заходи для блокування зовнішнього доступу через Internet до інформаційних ресурсів Комунального

закладу «Бахмутський медичний фаховий коледж», не призначених для публічного доступу, а також для захисту конфіденційної інформації при її передачі через Internet.

Відповідальний за інформаційну безпеку контролює виконання заходів із безпечного використання Internet, в межах приміщень, де здійснюється діяльність закладу освіти, а саме:

- контролює щоб доступ до Internet з робочих місць здійснювався через встановлені точки доступу до Internet;
- контролює, щоб тільки публічна та відкрита інформація про заклад освіти була доступна в Internet; здійснює моніторинг інформації, що розміщена на сайті коледжу;
- контролює, щоб користувачі не мали прав встановлювати або завантажувати будь-яке програмне забезпечення (додатки, медіа файли, заставки тощо) з Internet на службові комп'ютери. Якщо у користувачів є потреба в додатковому програмному забезпеченні, користувач повинен отримати дозвіл;
- використання Internet повинно узгоджуватися з діяльністю закладу освіти. Мережа не може бути використана для продажи сторонніх послуг (не передбачених діяльність та дозвільними документами Комунального закладу «Бахмутський медичний фаховий коледж»);
- використання мережі коледжу на робочому місці для отримання особистого прибутку заборонено;
- конфіденційні або персональні дані, включаючи номери кредитних карток, номери телефонів, паролі для входу в систему та інші дані, які можуть бути використані для доступу до конфіденційної або персональної інформації повинні передаватися через Internet у зашифрованому виді;
- передача КЕП та ЕЦП, які використовуються для ідентифікації співробітників коледжу у сервісах, що пов'язані з діяльністю закладу освіти, заборонено;
- використання програмного забезпечення для шифрування та ключів

шифрування повинно контролюватися відповідальним за ІБ. Самостійне використання шифрувального програмного забезпечення та ключів шифрування, без погодження з відповідальним за ІБ, заборонено, і може призвести до дисциплінарного покарання.

Під час дистанційної або віддаленої роботи персонал самостійно має опікуватись доступом до мережі Internet. При цьому, необхідно враховувати всі положення та норми, що описані в діючій ПІБ Комунального закладу «Бахмутський медичний фаховий коледж». Співробітники повинні вжити всіх заходів щодо збереження конфіденційності та цілісності службової інформації. Наприклад, у разі виконання службових завдань та обробки інформації, що стосується діяльності закладу освіти, заборонено використовувати публічні точки доступу до мережі.

2.5. Повідомлення про несправності

Користувач повинні інформувати інженера-програміста (або іншу особу, що є відповідальною за ІТ напрямок роботи коледжу) про випадки, коли програмне забезпечення робочої станції не функціонує належним чином. Вказане правило стосується також власних комп’ютерів, що використовуються для забезпечення діяльності закладу освіти під час дистанційної роботи. Несправне програмне забезпечення становить ризик для інформаційної безпеки. Якщо користувач, або керівник користувача, підозрює зараження робочої станції вірусом, слід негайно вжити наступних заходів:

- припинити використання комп'ютера;
- не запускати на виконання ніяких команд, включаючи команду збереження даних;
- не закривати жодного з вікон або програм комп'ютера;
- не вимикати комп'ютер або периферійний пристрій на самому екрані;
- по можливості фізично відключити комп'ютер від мереж живлення та локальної мережи;
- повідомити про ураження робочої станції інженера-програміста та/або

відповідального за ІБ, вказавши ознаки незвичайної поведінки комп'ютера (блокування екрану, виникнення несподіваного доступ до системного диска, незвичайна реакція на команди тощо) і час, коли це було вперше помічено;

- повідомити про будь-які зміни у використанні апаратного чи програмного забезпечення, які передували несправності;
- не намагатися самостійно видалити підозрілий об’єкт.

Відповідальний з ІБ повинен вжити заходи для усуненням несправності, а також повідомити директора коледжу про результати цих дій з рекомендаціями щодо подальших кроків для запобігання подібних випадків у майбутньому.

2.6. Повідомлення про інциденти безпеки

Всі співробітники, який є користувачами інформаційних ресурсів закладу освіти або підрядники, які мають доступ до цифрових активів Комунального закладу «Бахмутський медичний фаховий коледж» зобов'язані повідомляти відповідального з ІБ про виявлені інциденти інформаційної безпеки. Користувач – це будь-яка особа, уповноважена на доступ до інформаційного ресурсу закладу. Користувачі несуть відповідальність за повсякденну практичну безпеку ресурсу, яким вони користуються. Користувачі повинні повідомляти про всі інциденти безпеки або порушення політики безпеки негайно своєму безпосередньому керівнику або відповідальному з інформаційної безпеки. При неможливості негайного повідомлення про інцидент безпеки вищевказаним особам, користувач повинен без зволікань проінформувати про інцидент будь-якого члена Робочої групи з інформаційної безпеки закладу, які вказані вище в цьому документі.

Реагування на повідомлення про інциденти інформаційної безпеки повинно бути якомога швидким. Кожен член Робочої групи з інформаційної безпеки повинен негайно вжити заходи відповідно до Плану реагування на інцидент інформаційної безпеки. Кожен інцидент повинен бути проаналізованим, щоб визначити, чи потрібно внесення необхідних змін в

існуючу систему управління інформаційною безпекою Комунального закладу «Бахмутський медичний фаховий коледж». Усі виявлені інциденти реєструються в журналі інцидентів інформаційної безпеки. Обов'язком відповідального за ІБ є організація та проведення навчання, щодо будь-яких змін у плані реагування на інциденти, які були зроблені в результаті розслідування інциденту.

Внутрішні порушення інформаційної безпеки повинні оперативно розслідуватися. У разі підозри на порушення законодавства, відповідальний з ІБ повинен звернутися до правоохоронних органів.

2.7. Передача конфіденційної інформації

Передача конфіденційної інформації може здійснюватися за допомогою засобів електронного зв’язку, на цифрових носіях чи у паперовому виді. Конфіденційна інформація передається від однієї особи іншій під час ведення службових справ. Особа, яка отримала конфіденційну інформацію повинна забезпечити її зберігання відповідно до умов, встановлених особою, що надала таку інформацію. Всі співробітники закладу освіти повинні розуміти про чутливий характер персональних даних, що отримує заклад освіти в ході свого функціонування, і утримуватись від розголошення таких даних. Будь-яке цілеспрямоване оприлюднення конфіденційних даних, до яких співробітник має доступ, є порушенням, яке призведе до покарання, а також може призвести до судового позову стосовно порушника. Співробітники, які за своїми посадовими обов’язками мають доступ до конфіденційних даних здобувачів освіти або даних діяльності коледжу, мають проходити навчання щодо захисту конфіденційних та персональних даних відповідно графіку, затвердженого директором коледжу.

2.8. Передача даних та програмного забезпечення

Власне програмне забезпечення, яке не дозволене до використання в закладі, не може використовуватися на робочих станціях чи комп'ютерах або в локальній мережі Комунального закладу «Бахмутський медичний фаховий коледж». Якщо існує потреба в конкретному програмному забезпеченні,

потрібно надати запит на дозвіл своєму безпосередньому керівнику. Користувачі не повинні використовувати програмне забезпечення, що встановлене на робочих станціях, або на особистих комп'ютерах чи комп'ютерному обладнанні при дистанційній роботі без відповідного дозволу. Винятком можуть стати особисті комп’ютери, які використовуються під час дистанційної або віддаленої роботи, але працюють з інформаційними базами, доступ до яких надається у вигляді on-line сервісу з відповідною ідентифікацією користувача та має власні інструменти захисту даних. Наприклад, Єдина державна електрона база освіти, редагування якої здійснюється через web-інтерфейс, захистом якої опікуються ДП «Інфоресурс».

Дані, що є власністю Комунального закладу «Бахмутський медичний фаховий коледж» включаючи інформацію про здобувачів освіти, інформацію про ІТ-системи, фінансову інформацію або дані про людські ресурси, не повинні розміщуватися на будь-якому комп'ютері, який не є власністю коледжу, без письмової згоди відповідного керівника. Заклад освіти повинен захищати всі дані та програмне забезпечення, які йому належать, тому повинен контролювати системи, в яких такі дані містяться. У випадку, якщо директор отримає від співробітника запит на переміщення даних з робочої станції на особистий ПК, керівник повинен визначитися чи є в цьому службова потреба та уразі прийняття рішення на дозвіл переміщення, повідомити відповідального з інформаційної безпеки про таку передачу даних. При цьому необхідно вживати додаткових заходів щодо забезпечення цілісності інформації, таких як додаткове резервне копіювання.

Треба розуміти, що заклад обмежений у можливостях захисту даних на особистих комп’ютерах, тому дозвіл на переміщення треба надавити у разі гострої службової необхідності, такої як – дистанційна робота. Заклад не може бути впевнений у засобах, які можуть бути застосовані для захисту конфіденційної чи чутливої інформації на особистих комп’ютерах, звідси необхідність цього обмеження.

2.9. Шифрування електронної пошти та даних

Для забезпечення конфіденціальної та захисту конфіденційної інформації при передачі в мережі Internet дозволяється використання відповідного програмного забезпечення (наприклад програми WinZip), яке дозволяє персоналу обмінюватися електронною поштою з віддаленими користувачами, які теж мають відповідне програмне забезпечення для шифрування/ дешифрування. Обидва користувачі обмінюються таємними паролями (у випадку використання WinZip) або відкритими ключами, які можуть бути використані для дешифрування повідомлення. Співробітник, який бажає використати відповідне програмне забезпечення повинен звернутися до відповідального за ІБ для отримання дозволу на використання відповідного програмного забезпечення.

При передачі конфіденційної інформації електронною поштою та розумінні, що є ризик потрапляння такої інформації до сторонніх осіб чи отримання доступу до неї сторонніми особами необхідно застосовувати програмне забезпечення шифрування/дешифрування (наприклад WinZip).

Вся персональна інформація та дані яка зберігаються на робочих станціях Комунального закладу «Бахмутський медичний фаховий коледж» повинні бути в зашифрованому вигляді. До такої інформації відноситься будь-яка інформація, яка може бути використана для ідентифікації особи, а саме:

- імена та прізвища;
- адреси;
- всі елементи дат, безпосередньо пов'язаних з особою (дати народження, дати вступу до закладу освіти, дати завершення навчання та ін.);
- телефонні номери;
- адреси електронної пошти;
- серії та номери документів, що засвідчують особу;
- серії та номери документів про освіту;
- персональні медичні дані: довідки, інформації про щеплення здобувачів освіти, данні медичних книжок працівників;

- номери банківських рахунків співробітників та студентів, отримувачів стипендій;
- ідентифікатори пристроїв і серійні номери;
- IP-адреси web-сайту закладу освіти;
- фотографічні зображення обличчя.

3. УПРАВЛІННЯ ДОСТУПОМ

3.1. Ідентифікація користувачів

В залежності від інформаційної бази Комунального закладу «Бахмутський медичний фаховий коледж», до якої отримується доступ, кожний користувач повинен мати унікальний ідентифікатор (обліковий запис, логін) та пароль для входу. Система контролю доступу повинна ідентифікувати кожного користувача і запобігати доступу та використанню інформаційних ресурсів закладу неавторизованим користувачем. Вимоги безпеки для ідентифікації користувача включають:

- кожному користувачеві присвоюється унікальний ідентифікатор;
- користувачі несуть відповідальність за використання та неправомірне використання свого індивідуального ідентифікатору.

Зазначені правила стосуються внутрішньої мережі закладу освіти, тимчасових VPN з'єднань та ідентифікації користувачів на платформах on-line освіти. Усі ідентифікатори входу користувачів перевіряються щонайменше раз на рік і всі неактивні ідентифікатори блокуються. Відділ кадрів та навчальна частина коледжу сповіщає відповідального за ІБ або відповідного фахівця інженера-програміста про звільнення співробітника або відрахування здобувача освіти (у випадках ідентифікації на платформах on-line освіти). При отримані такого сповіщення неактивні ідентифікатори блокуються.

Блокування ідентифікаторів користувачів, у разі неправильних спроб введення паролів, блокуються відповідно до правил сервісів, що

використовуються (ЄДЕБО, G Suite for Education та ін.) та відповідають їх ПІБ. Користувачі отримують доступ до ідентифікації в інформаційних базах та сервісах, що забезпечують діяльність коледжу, виключно відповідно до своїх посадових обов’язків або (у випадку зі студентами на платформах on-line освіти) відповідно до академічної групи.

3.2. Встановлення паролів

Ідентифікатори користувачів і паролі потрібні для того, щоб отримати доступ до мереж і робочих станцій. До всіх паролів застосовується встановлена цім документом Парольна політика, для забезпечення стійкості паролів. Це означає, що всі паролі повинні відповідати вимогам, які призначені для того, щоб пароль було важко підібрати чи зламати. Користувачі зобов'язані створювати та користуватися паролями, щоб отримати доступ до відповідних мереж, ІТ-ресурсів, баз даних, сервісів чи робочої станції. При призначені паролю користувачеві буде автоматично запропоновано вручну призначити пароль, відповідно до таких вимог:

- довжина пароля – пароль повинен складатися з мінімуму десять (10) символів;
- вимоги до складу – пароль повинен містити комбінацію символів латинського алфавіту верхнього та нижнього регістру, числових символів та спеціальних символів;
- частота зміни – Пароль повинен бути змінений кожні 60 днів. Скомпрометований пароль повинен бути змінений негайно;
- повторне використання – попередні три (3) паролі не можуть бути використані повторно;
- обмеження на обмін паролями – паролі не повинні передаватися іншим співробітникам чи іншим здобувачам освіти, записуватися на папері або зберігатися на робочій станції;
- обмеження на відображення та зберігання паролів – паролі маскуються на екрані робочої станції при введені, не друкуються і не включаються до

електронних журналів чи звітів. Паролі зберігаються у зашифрованому виді.

Зазначені правила стосуються і паролів, що задаються для КЕП та ЕЦП, які використовуються для доступу до електронних баз і сервісів з відповідним способом ідентифікація користувачів.

3.3. Угода про конфіденційність

Користувачі інформаційних ресурсів освіти, які відповідно до своїх посадових обов'язків мають доступ до персональних даних, даних фінансової та господарської діяльності або іншої інформації, яка відносить до конфіденційної, при працевлаштуванні підписують угоду про конфіденційність (Додаток 2). Угода повинна містити наступне твердження:

Я розумію, що будь-яке несанкціоноване використання або розголошення конфіденційної інформації, може призвести до покарання, відповідно до чинного законодавства та політики інформаційної безпеки.

Тимчасово влаштовані працівники, які не підписували угоди про конфіденційність, підписують такий документ при отримані доступу до інформаційних ресурсів коледжу, які можуть містити таємницю.

Угода про конфіденційність переглядається, коли відбуваються зміни умов трудової діяльності, зокрема при звільнені співробітника або суттєвій зміні посадових обов'язків.

3.4. Контроль доступу

В закладі можуть використовуватись випливаючи на екрані робочих станцій електронні попередження про несанкціоноване використання ресурсу та про відповідальність порушника.

При використанні програмного забезпечення управління безпекою кінцевих пристроїв повинна підтримуватися on-line авторизації при використані додатків. Кожне підключення підлягає процесу авторизації (введенню логіна та пароля). В коледжі може використовуватись віддалене адміністрування або

перегляд робочих станцій з боку ВІБ, директора або керівника підрозділу (головного бухгалтера, заступника директора з навчальної роботи та ін.). Вданому випадку використовується відповідне програмне забезпечення, яке має відповідати засадам цієї ПІБ.

3.5. Припинення права доступу

Якщо співробітник змінює посаду або набуває нових повноважень чи обов'язків – його керівник (безпосередній керівник відповідно до адміністративної структури коледжу) ініціює перегляд прав доступу та заповнює Форму запиту на доступ (Додаток 1). У Формі вказується дата набрання чинності зміни посади, для зміни права доступ відповідно до принципу мінімально необхідного доступу до ресурсів. Протягом обмеженого періоду у співробітника, який змінює посаду (або набуває чи втрачає повноваження), можуть зберігатися попередні права доступу, а також додаватися нові права доступу, необхідні для виконання нових посадових обов'язків.

Перегляд прав доступу повинен проводитися не рідше ніж раз на рік. Відповідальний за інформаційну безпеку повинен сприяти перегляду прав доступу користувачів, щоб переконатися, що весь персонал має мінімально необхідні права доступ для ефективного виконання своїх робочих функцій. Виявлені в ході перегляду надлишкові права доступу повинні припинятися.

3.6. Припинення дії облікового запису користувача

При звільненні працівника або втрати певних повноважень на доступ до інформації, його безпосередній керівник повинен завчасно ініціювати процедуру припинення доступу, вказавши «Видалити доступ» у Формі запиту на доступ (Додаток 1) та дату останнього дня, коли співробітник має права на доступ, щоб його обліковий запис користувача міг бути налаштований на закінчення терміну дії у день звільнення. Безпосередній керівник контролює своєчасну здачу працівником, що звільняється відповідних пристрої доступу, які йому/їй надавалися (пристрої для зчитування токенів або ін). Обліковий запис та доступ

працівника блокується по завершені останнього робочого дня.

Не рідше одного разу на рік, відповідальний з інформаційної безпеки повинен ініціювати перегляд списку активних облікових записів користувачів для оцінки прав доступу відповідно до принципу надання мінімально необхідного доступу до ІТ-ресурсів для виконання функціональних завдань. Про необхідність припинення надлишкових прав доступу або блокуванні активних акаунтів звільнених працівників невідкладно повідомляється ВІБ, який в свою чергу без зволікань повідомляє відділ (сектор, підрозділ або відповідного інженера) та надає оновлену Форму запиту на доступ (Додаток 1). Зазначені правила стосуються виключно фінансової або господарської діяльності Комунального закладу «Бахмутський медичний фаховий коледж» та діяльності, що пов’язана з обробкою персональних даних. Видалення облікових записів здобувачів освіти з платформ on-line навчання здійснюється без заповнення Форми, списком за подачею навчальної частини – особою, що відповідальна за даний напрямок.

4. ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ

4.1. З'єднання та підключення

Доступ до інформаційних ресурсів Комунального закладу «Бахмутський медичний фаховий коледж» здійснюється локально або через Internet з'єднання (у разі звернення до on-line сервісів або через програмне забезпечення, яке вимагає Internet з'єднання). При організації доступу до мережі в межах будівлі коледжу використовуються роутери або інші телекомунікаційні пристрої. Зовнішня комутація на ресурси, що знаходяться на робочих станціях – блокується. Під час дистанційної або віддаленої роботи, співробітники коледжу зобов'язані дотримуватись вимог інформаційної безпеки та вжити всіх заходів щодо забезпечення конфіденційності та цілісності даних, які стосуються діяльності Комунального закладу «Бахмутський медичний фаховий коледж». В межах будівлі коледжу організовуються однорангова локальна мережа, блокування зовнішніх загроз в якій здійснюється на кожній робочій станції окремо. Системи, що дозволяють проходження зовнішнього виклику на кінцевий пристрій повинні гарантувати додаткову безпеку на рівні операційної системи та додатків. Такі системи повинні також мати можливість контролювати рівень активності, щоб гарантувати, що використання кінцевих пристроїв відбувається належним чином та з виконанням заходів безпеки.

Права доступу до з'єднання через комутатори або роутери надаються тільки на вимогу керівника підрозділу (головний бухгалтер, начальник відділу кадрів та ін.) з поданням Форми доступу (Додаток 1) та погоджуються з директором коледжу чи відповідальним за ІБ.

Підключення до зовнішніх мереж відбувається через інтернет-провайдера. Якщо користувач має конкретну потребу зв'язатися із зовнішнім комп'ютером або мережею через прямий канал зв’язку він повинен отримати дозвіл від керівника закладу освіти. При прийняті позитивного рішення відповідальний з інформаційної безпеки повинен вжити необхідних заходів із забезпечення належного рівня безпеки нового каналу зв’язку.

4.2. Телекомунікаційне обладнання

До телекомунікаційного обладнання та засобів відноситься наступне:

- телефонні лінії та обладнання;
- службові мобільні телефони;
- програмне забезпечення для маршрутизації викликів;
- обладнання для адміністрування;
- мережеві лінії;
- місцеві телефонні лінії.

Цей перелік не є вичерпним.

4.3. Постійні з’єднання

Забезпечення безпеки телекомунікаційних з’єднань є дуже важливим завданням. Інформаційна безпека закладу може бути поставлена під загрозу, якщо не забезпечити безпечне користування засобами зв’язку. Необхідно забезпечити аналіз ризиків при підключені до зовнішніх мереж та регулярно аналізувати ризики постійно діючих каналів з’єднання. Аналіз ризиків повинен враховувати тип необхідного доступу, цінність інформації що передається, заходи безпеки, що застосовуються третьою стороною, а також наслідки для системи управління безпекою закладу. Відповідальний за інформаційну безпеку повинен бути залучені до процесів проектування та затвердження каналів підключення до зовнішніх мереж, а також укладення договорів з третьою стороною на отримання послуг з телекомунікаційного забезпечення закладу.

4.4. Договір на телекомунікаційні послуги

При укладанні договору на отримання телекомунікаційних послуг закладом необхідно враховувати наступні вимоги до постачальника таких послуг:

- відповідні розділи політики інформаційної безпеки надавача послуг були переглянуті та приведені у відповідність з вимогами політики інформаційної безпеки закладу;
- відповідні вимоги враховані та застосовуються;
- проведена оцінка ризиків пов’язаних з виконанням додаткових зобов'язань надавача послуг;
- включене право на аудит виконання договірних зобов’язань;
- домовленість стосовно повідомлення про інциденти інформаційної безпеки включені в угоду;
- наданий опис кожної послуги, яка буде доступна;
- доступ до ресурсів закладу надавачем послуг повинен бути лише на мінімально необхідному рівні, достатньому для виконання договірних зобов'язань;
- детальний список користувачів з боку надавача послуг, які будуть мати доступ до мережі закладу, повинен бути доступний для аудиту;
- дата і час, коли послуга повинна бути доступна, завчасно узгоджені;
- процедури щодо захисту інформаційних ресурсів узгоджені заздалегідь, а спосіб аудиту затверджений обома сторонами;
- спосіб моніторингу і припинення доступу користувачів визначений;
- обмеження на копіювання та розкриття інформації включені;
- обов'язки щодо встановлення та технічного обслуговування апаратного та програмного забезпечення зрозумілі та заздалегідь узгоджені;
- заходи щодо забезпечення повернення або знищення програмного забезпечення та інформації після закінчення дії договору визначені та прописані;
- заходи фізичного захисту, при необхідності, також включені в угоду;

- створені механізми для забезпечення дотримання заходів безпеки сторонами угоди;
- детальний перелік заходів безпеки, які будуть вжиті сторонами угоди, повинен бути розглянутий та погоджений до укладення угоди.

У разі самостійного забезпечення доступу до мережі Internet під час дистанційної роботи закладу освіти, кожен співробітник, що працює з чутливою інформацією повинен враховувати загальні вимоги до надавачів послуг Internet доступу. В такому випадку, співробітники коледжу несуть персональну відповідальність за збереження даних, що можуть бути втраченими, оприлюдненими чи скомпрометованими.

4.5. Брандмауер

Налаштування брандмауера повинно контролюватися відповідальним з ІБ. Якщо брандмауер знаходиться та налаштовується стороною, яка надає ІТ-послуги закладу освіти (провайдера) то ця сторона повинна надати повну інформацію про актуальні налаштування брандмауера відповідальному за інформаційну безпеку та активно співпрацювати з ним/нею у питаннях подальшого його використання та змін налаштувань. Під час дистанційної або віддаленої роботи, співробітники, що працюють з чутливою інформацією Комунального закладу «Бахмутський медичний фаховий коледж» в обов’язковому порядку повинні використовувати програмні засоби захисту інформації (брандмауер, мережевий екран та ін.) та на вимогу відповідального за ІБ повідомляти інформацію про ці засоби. У разі недотримання вимог щодо використання зазначеного програмного захисту – співробітник може бути позбавлений права доступу до інформаційних баз коледжу з особистого пристрою.

5. АНТИВІРУСНИЙ ЗАХИСТ

5.1. Встановлення та оновлення антивірусного програмного забезпечення

Антивірусне програмне забезпечення встановлюється на всіх робочих станціях Комунального закладу «Бахмутський медичний фаховий коледж» та періодично (відповідно до офіційних оновлень постачальника) оновлюється. За своєчасне оновлення антивірусного програмного забезпечення відповідає інженер-програміст.

Конфігурації – антивірусне програмне забезпечення, яке на даний час використовується в Комунальному закладі «Бахмутський медичний фаховий коледж» - є Free Avast Antivirus . Оновлення надходять безпосередньо від NortonLifeLock. Оновлення відбувається автоматично.

Конфігурація віддаленого розгортання – встановлення антивірусного програмного забезпечення в закладі відбувається виключно при безпосередній роботі з робочою станцією.

Моніторинг/Звітність – в закладі ведеться контроль оновлення та застосування антивірусного програмного забезпечення. Інженер-програміст несе відповідальність за надання звітів про перевірку спрацювання антивірусного програмного забезпечення при інцидентах інформаційної безпеки.

Під час дистанційної або віддаленої роботи співробітники коледжу в обов'язковому порядку повинні використовувати антивірусне програмне забезпечення під час роботи із чутливою інформацією Комунального закладу «Бахмутський медичний фаховий коледж».

5.2. Перевірка нового програмного забезпечення

На внутрішніх комп'ютерах і мережі коледжу використовується лише дозволене до використання програмне забезпечення. Встановлення нового програмного забезпечення потребує отримання дозволу керівника закладу або відповідального з інформаційної безпеки. Перелік дозволеного до використання програмного забезпечення наведений у Додатку 3. Перед встановленням нове програмне забезпечення проходить перевірку інженером-програмістом з метою забезпечення сумісності зі встановленим на даний момент програмним забезпеченням і конфігурацією мережі. Крім того, інженер-програміст повинен перевірити нове програмне за допомогою наявного антивірусного програмного забезпечення на наявність вірусів та інших шкідливих програм перед установкою. Це стосується як програмного забезпечення, що закуповується так і умовно-безкоштовного програмного забезпечення.

Хоча умовно-безкоштовне програмне забезпечення може бути корисним, використання такого програмного забезпечення має бути попередньо схвалено відповідальним з інформаційної безпеки. Оскільки програмне забезпечення часто завантажуються з загальнодоступного джерела та може мати віруси та інше шкідливе програмне забезпечення, перед його встановленням на комп'ютерах коледжу необхідно вжити спеціальних запобіжних заходів. Ці запобіжні заходи включають визначення того, що програмне забезпечення є сумісним з існуючим ПЗ, не перешкоджає або не пошкоджує апаратне забезпечення, програмне забезпечення або інформацію, а також що програмне забезпечення не містить вірусів та інших шкідливих програм. Всі файли і програми, які були передані в електронному вигляді на комп'ютери або мережу закладу з іншого місця, повинні бути перевірені на віруси відразу після отримання. Перевірку та сканування на віруси здійснює інженер-програміст за допомогою наявного антивірусного програмного забезпечення. Кожна дискета, компакт-диск, DVD і USB-пристрій є потенційним джерелом комп'ютерного вірусу. Тому такі зовнішні носії інформації повинні бути про скановані на наявність вірусів та іншого шкідливого програмного забезпечення, перш ніж інформація з них буде скопійована на

комп'ютери закладу. Забороняється завантажувати комп'ютери з дискети, компакт-диска, DVD або USB-пристрою, отриманого із зовнішнього джерела. Користувачі завжди повинні видаляти будь-яку зовнішні носії з комп'ютера, коли він не використовується.

5.3. Збереження прав власності

Усі програмні продукти та документація, що надаються співробітникам власністю закладу, якщо на них не поширюється дія іншого договору. Програмні засоби, застосунки або документація які розробляються за замовленням закладу є також його власністю. Розробники таких програмних продуктів та документації повинні підписати заяву, в якій визнається право власності закладу на відповідний програмний продукт та документацію. Програмне забезпечення, придбане працівником за власний рахунок, залишається власністю працівника, який придбав це програмне забезпечення.

6. КРИПТОГРАФІЧНИЙ ЗАХИСТ

6.1. Визначення

Криптографічний захист інформації за допомогою шифрування даних є найефективнішим способом забезпечення безпеки даних Комунальний заклад «Бахмутський медичний фаховий коледж».

Шифрування це процес перетворення інформації, використовуючи криптографічний алгоритм, щоб зробити її нечитабельною для будь-кого, крім тих, хто має авторизовану «потребу знати». Щоб отримати доступ до зашифрованої інформації, необхідно мати доступ до секретного ключа або паролю, що дозволяє його розшифрувати. В закладі використовуються наступні засоби криптографічного захисту: інфраструктура відкритих ключів з електронним цифровим підписом; програма – архіватор WinZip; передача даних через захищений протокол SSL та веб-інтерфейс HTTPS.

Криптографічний захист інформації, що передається обробляється та зберігається в інформаційних системах коледжу забезпечується провайдером, відповідно до вимог, що зазначені в частині 4 даної ПІБ.

6.2. Ключі шифрування

Ключ шифрування визначає особливе перетворення простого тексту у зашифрований, або навпаки під час дешифрування (розшифрування). Якщо це обґрунтовано аналізом ризиків інформаційної безпеки, конфіденційні дані та файли, що містять конфіденційну інформацію, повинні бути зашифровані перед передачею через мережу загального користування чи Internet. Коли зашифровані дані передаються між закладом та сторонньою організацією необхідно

розробити та запровадити взаємну процедуру обміну та безпечного управління ключами. У разі виникнення інциденту, пов’язаного з криптографічним захистом інформації, його вирішенням повинен займатися відповідальний з інформаційної безпеки закладу. Заклад може використовувати декілька методів безпечної передачі даних за допомогою криптографічного захисту.

6.3. Використання інфраструктури відкритих ключів

Користувач, який має потребу у безпечній передачі інформації електронною поштою конкретному ідентифікованому зовнішньому користувачеві, може скористатися інфраструктурою відкритих ключів та електронним цифровим підписом (ЕЦП) або кваліфікованим електронним підписом (КЕП). Порядок використання ЕЦП та КЕП у закладі освіти повинно бути погоджено з керівником чи відповідальним за інформаційну безпеку.

6.4. Використання WinZip

WinZip – це програмне забезпечення дозволяє персоналу закладу обмінюватися електронною поштою з віддаленими користувачами, які мають відповідне програмне забезпечення для шифрування та дешифрування. Обидва користувачі обмінюються паролем, який використовується як для шифрування, так і для дешифрування/розшифрування кожного повідомлення. Пароль передається отримувачу альтернативним засобом зв'язку, таким як смс, месенджер або телефоном. Працівник, який має потребу у передачі конфіденційної інформації віддаленому користувачу через Internet може запросити дозвіл на використання програми WinZip у відповідального з інформаційної безпеки. При цьому відповідальний з ІБ повинен також отримати пароль до зашифрованого архіву для перевірки інформації, що підлягає передачі чи отримується.

6.5. Веб-інтерфейс рівня захищених сокетів (SSL)

Для передачі конфіденційної інформації через веб-інтерфейсі

використовується веб-інтерфейс захисту SSL. SSL (англ. Secure Sockets Layer) - криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і веб-сервером. Протокол забезпечує конфіденційність обміну даними між клієнтом і сервером, що використовують TCP/IP. Користувач через веб-інтерфейс захисту SSL передає/отримує конфіденційну інформації через веб-сторінку в Інтернеті при наданні/отриманні послуг онлайн. Порядок використання веб- інтерфейсу захисту SSL погоджується з керівником закладу освіти та відповідальним з інформаційної безпеки.

7. ФІЗИЧНА БЕЗПЕКА

Забезпечення фізичної безпеки персоналу полягає у створені безпечних умов на робочому місці та одночасним забезпеченням безпечного зберігання активів закладу. Будівля (комплекс будівель або частина будівлі) закладу є дещо унікальним місцем з точки зору прав власності на будівлю або умов договору оренди, території навколо, шляхів під'їзду/виїзду, зовнішнього огородження, входів у приміщення, вимог до пожежної безпеки, систем електроживлення, забезпечення безпечного використання цифрових активів та контролю кабінетів, де розміщено комп'ютерне обладнання. Необхідно постійно покращувати та модернізувати систему забезпечення фізичної безпеки для підвищення захисту своїх активів та інформації, з якою працює заклад освіти. Наступний перелік визначає заходи, які запроваджені для забезпечення фізичної безпеки закладу освіти.

Вхід до будівлі в неробочий час зачинені. Спроба входу сторонньої особи без попереднього узгодження з адміністрацією тягне за собою виклик поліції. В коледжі наявні наступні засади фізичної безпеки:

- тільки конкретним працівникам закладу надається вхід до будівель;
- вхідні двері в будівлю, де проводить свою діяльність заклад освіти, завжди замикаються у неробочий час і відмикаються у робочі години закладу;
- будь-яка невизнана особа, яка перебуває в службових приміщеннях закладу повинна негайно виводитись з службової зони персоналом, що її побачив;
- робочі станції, ноутбуки, телефоні апарати інше цифрове обладнання, яке

знаходиться в зоні дозволеної для знаходження відвідувачів, повинні бути облаштовані спеціальними їх фізичного збереження, що унеможливлює винос або переміщення від встановленого місця розташування.

До приміщень де знаходиться комп'ютерне обладнання вхід заблоковано вхідними металевими дверима, на вікнах встановлено решітки.

Протипожежний захист будівлі встановлено відповідно до вимог ДСНС України.

Під час впровадження дистанційної роботи закладу освіти, у разі використання обладнання, що є активом Комунального закладу «Бахмутський медичний фаховий коледж» або під час використання особистого обладнання, що обробляє інформацію, яка належить зазначеному закладу освіти, співробітники самостійно зобов'язані вжити заходів з метою збереження зазначеного обладнання. У разі втрати або всування обладнання, співробітник несе фінансову відповідальність за випадок. У разі втрати активів Комунального закладу «Бахмутський медичний фаховий коледж» через дії третіх осіб, співробітник зобов'язаний одразу повідомити керівника закладу, відповідального за ІБ та звернутись з заявою до Національної Поліції.

8. ДИСТАНЦІЙНА РОБОТА

В закладі дозволяється та використовується дистанційна робота персоналу при певних, визначених керівництвом обставинах. Дистанційна робота в Комунальному закладу «Бахмутський медичний фаховий коледж» впроваджується прямим наказом директора коледжу і може стосуватись як окремих співробітників, так і закладу в цілому. На момент затвердження даної ПІБ Комунальний заклад «Бахмутський медичний фаховий коледж» здійснює свою діяльність с дистанційному режимі.

Вимоги, щодо організації дистанційної роботи застосовуються до всіх співробітників, які працюють поза межами будівлі (комплексу будівель або частини будівлі) закладу.

Хоча дистанційна робота може бути перевагою як для здобувачів освіти, так і для закладу в цілому, вона представляє нові ризики інформаційної безпеки. Співробітники та викладачі коледжу, що працюють дистанційно повинені бути захищеними від небезпеки атак шкідливим програмним забезпеченням та несанкціонованого витоку даних з пристроїв, що знаходяться за межами периметру безпеки закладу.

8.1. Загальні вимоги

Користувачі, що працюють віддалено, зобов'язані дотримуватися всіх правил закладу, які встановлені для співробітників та викладачів Комунального закладу «Бахмутський медичний фаховий коледж».

Потрібно знати:

- користувачі, що працюють віддалено мають доступ тільки до тих ресурсів та інформації, які потрібні для виконання їх функціональних завдань та обов’язків;
- користувачі, що працюють віддалено повинні дотримуватись вимог щодо встановлення та зміни паролів; окрім того, вони не розголошують свій пароль і не залишають записів щодо паролю там, де такий запис може побачити член сім'ї або стороння особа;
- співробітники, які працюють віддалено, повинені проходити ті самі навчання з інформаційної безпеки, що і ті що працюють на робочих місцях.
- до співробітників, що працюють віддалено, можуть бути застосовані додаткові вимоги, які пов’язані зі специфікою виконання функціональних завдань дистанційно.

8.2. Необхідне обладнання

Співробітники, допущені до дистанційної роботи, повинні розуміти, що заклад не наддасть все обладнання, необхідне для забезпечення належного захисту інформації, до якої працівник має доступ; однак є певний перелік обладнання який заклад може надати за прямою вказівкою або розпорядженням директора:

- робочий комп’ютер (ноутбук) зі встановленим антивірусним ПЗ та програмним забезпеченням шифрування даних;
- принтер;
- зовнішній носій для резервного копіювання;
- службовий мобільний телефон.

Надання зазначених пристроїв для використання поза межами будівель коледжу є припустимим, але не обов’язковим. Кожен випадок розглядається окремо, в залежності від обсягу роботи та переліку посадових обов’язків. Працівник повинен забезпечити самостійно:

- широкосмуговий канал доступу до Інтернет;
- подрібнювач паперу або можливість іншим способом знищувати паперові

носії;

- відокремлене від членів родини робоче місце;
- шафа, що зачиняється або сейф для захисту та зберігання робочого комп’ютера та робочих документів.

Викладачі, під час дистанційної роботи закладу, самостійно забезпечують себе необхідною технікою та обладнанням для проведення навчальної та методичної роботи. При цьому, викладачі мають усвідомлювати, що працюють з персональними даними здобувачів освіти, тому повинні максимально дотримуватись вимог, що описані в ПІБ Комунальному закладу «Бахмутський медичний фаховий коледж».

8.3. Захист апаратного забезпечення

Захист від вірусів. Користувач, що працює дистанційно, повинен постійно використовувати та оновлювати захист комп’ютера від вірусів та іншого шкідливого програмного забезпечення. Антивірусне програмне забезпечення встановлене на комп'ютерах закладу і налаштоване на періодичне оновлення. Заборонено працювати без оновленого антивірусного програмного забезпечення.

Використання VPN та брандмауера. При дистанційному підключені повинен використовуватись канал зв’язку, який вимагає використання VPN та брандмауера. При відключені VPN та/або брандмауера дистанційну роботу потрібно зупинити.

Шафа або сейф. Використовуйте шафу, що замикається або сейф для безпечного зберігання комп’ютеру та інших пристроїв наданих закладом для дистанційної роботи.

Захист ПК. Персональний комп’ютер, що використовується для дистанційної роботи, повинен бути облаштований спеціальним замком для захисту від крадіжки.

Блокування екранів. Незалежно від місця розташування, завжди блокуйте екран, перш ніж відійти від робочої станції. Дані на екрані можуть містити

конфіденційну інформацію. Переконайтеся, що функцію автоматичного блокування настроєно на автоматичне ввімкнення після 10 хвилин бездіяльності.

8.4. Безпека даних

Резервне копіювання даних. Встановлена процедура резервного копіювання, яка шифрує дані, та переміщує їх на зовнішній носій. Для резервного копіювання використовується тільки встановлена процедура. Створювати самостійно інші процедури резервного копіювання даних заборонено. Якщо неможливо дотримуватись встановленої процедури резервного копіювання: не має відповідного програмного забезпечення та/або зовнішнього носія, треба звернутися до інженера-програміста закладу або відповідального за ІБ. При гострій необхідності та неможливості звернутися до зазначених осіб (наприклад під час відрядження) дозволено використовувати наявні засоби шифрування (архіватор-шифрувальник WinZip) та доступний зовнішній носій. Причому, безпечному зберіганню зовнішнього носія з резервною копією даних треба приділити значну увагу.

Передача даних. Передача даних до закладу бажана з використанням затвердженого VPN-з'єднання для забезпечення конфіденційності та цілісності даних, що передаються. Не дозволено обходити встановлену процедуру, а також створювати власний метод передачі даних до закладу.

Доступ до зовнішніх систем (хмар). Якщо є потреба у доступі до зовнішньої ІТ-системи, необхідно зв'язатися зі своїм безпосереднім керівником або відповідальним за інформаційну безпеку. Вони визначать безпечний метод доступу до потрібної зовнішньої системи.

Електронна пошта. Не дозволено передавати будь-яку конфіденційну інформацію та персональні дані (перелік визначений у п.2.9 цього документу) електронною поштою, якщо вона не зашифрована. При гострій необхідності треба звернутися до свого безпосереднього керівника або відповідального за інформаційну безпеку. Вони визначать безпечний метод передачі конфіденційної інформації та персональних даних електронною поштою.

Захистить дані, якими ви володієте. Потрібно отримувати доступ лише до тієї інформації, яка потрібна для виконання робочого завдання. Регулярно переглядайте дані, які ви зберегли, щоб переконатися, що масив даних, який зберігається знаходиться на мінімально необхідному рівні, а застарілі дані та версії файлів видалені. Зберігайте електронні дані тільки в зашифрованому виді. Якщо на ноутбуку не встановлено відповідне ПЗ для шифрування треба звернутися до інженера-програміста закладу освіти.

Друковані звіти або робочі документи. Ніколи не залишайте паперові документи на робочому столі коли ви залишаєте робоче місце. Всі паперові документи повинні зберігатися у замкненій шафі або сейфі.

Введення даних у відкритому місці. Не виконуйте робочі завдання, які вимагають використання конфіденційної інформації або персональних даних у громадських місцях.

Надсилання даних за межи закладу. Вся передача даних за межі закладу повинна бути пов'язана з виконанням вимог договорів та дотримуватися вимог угод про конфіденційність і нерозголошення конфіденційної інформації. При необхідності передачі інформації стороннім організаціям з якими не укладено договорів та угод на обмін інформацією необхідно отримати письмову згоду безпосереднього керівника.

8.5. Утилізація паперових та зовнішніх носіїв

Паперові документи. Всі паперові документи, які містять конфіденційну інформацію, перед утилізацією потрібно подрібнити. Заборонено викидання не подрібнених паперових документів. Іншій спосіб утилізації - такі документи палити. Персонал, який працює дистанційно повинен мати або подрібнювач паперу або можливість палити паперові документи.

Зовнішні носії. Всі зовнішні носії надані закладом для забезпечення дистанційної роботи повинні бути повернуті до закладу для утилізації.

9. ПОЛІТИКА ЧИСТОГО СТОЛУ/ЕКРАНУ

Одним із засобів контролю за забезпечення інформаційної безпеки є політика чистого столу та чистого екрану, яка знижує ризик несанкціонованого доступу, втрату та пошкодження інформації протягом робочого часу та після його закінчення. Політика чистого столу та чистого екрану визначає методи, пов'язані із забезпеченням того, щоб конфіденційна інформація, як у цифровому, так і у паперовому/фізичному форматі, та активи (наприклад, робочі станції, ноутбуки, стаціонарні телефонні апарати, смартфони та інші) не залишаються без захисту, коли вони не використовуються, чи коли персонал залишає свої робочі місця на короткий час або наприкінці дня. Дотримання політики чистого столу/екрану всього без винятку персоналу дозволить суттєво убезпечити Комунальний заклад «Бахмутський медичний фаховий коледж» від витоку конфіденційної інформації.

Метою впровадження політики чистого столу та чистого екрану в Комунальному закладі «Бахмутський медичний фаховий коледж» є:

- запобігання витоку/втраті конфіденційних даних закладу;
- дотримання правил кібергігієни та розвитку кіберкультури, щодо безпечного та належного поводження з конфіденційною інформацією та її носіями;
- створення та підтримання позитивного іміджу закладу серед здобувачів освіти.

Вимоги цієї політики поширюються на всіх співробітників закладу. Усі співробітники, викладачі та здобувачі освіти закладу мають бути ознайомлені із

її вимогами. До будь-якого працівника закладу, визнаного винним у порушенні цієї політики, може бути застосована дисциплінарна практика, аж до звільнення.

Чистий стіл/екран є важливим аспектом інформаційної безпеки в закладах освіти. Він сприяє збереженню конфіденційності, забезпечує безпеку даних та підвищує продуктивність. Ключові пункти політики чистого столу/екрану:

1. Заборона зберігання конфіденційних даних на робочому столі/екрані. Всі конфіденційні дані (наприклад, паролі, особисті файли) повинні бути збережені в безпечних місцях, а не на робочому столі або на екрані.
2. Регулярне очищення робочого столу/екрану. Працівники повинні регулярно видаляти непотрібні файли та ярлики з робочого столу/екрану.
3. Обмеження використання особистих програм та файлів. Заборонено використовувати робочий стіл/екран для особистих цілей, таких як особисті фотографії, музика або інші приватні файли.
4. Підтримка безпеки даних. Працівники повинні дотримуватися політики безпеки даних, щоб уникнути витоку конфіденційної інформації через робочий стіл/екран.

Зазначені правила та вимоги обов’язкові до дотримання як під час роботи в будівлях коледжу, так і під час дистанційної або віддаленої роботи.

Комунальний заклад «Бахмутський медичний фаховий коледж» Політика інформаційної безпеки	
Назва: УТИЛІЗАЦІЯ ЗОВНІШНІХ НОСІЇВ ТА КОМП'ЮТЕРІВ	п.10.1-10.3
Дата затвердження 30.05.2024 Дата набрання чинності: 01.06.2024	Огляд: Щорічний Інформаційна безпека закладів освіти; Інформаційна безпека закладів охорони здоров'я

10. УТИЛІЗАЦІЯ ЗОВНІШНІХ НОСІЇВ ТА КОМП'ЮТЕРІВ

10.1. Утилізація зовнішніх носіїв

Вважається, що всі зовнішні носії, які використовувались співробітниками Комунального закладу «Бахмутський медичний фаховий коледж» містять конфіденційну та/або медичну інформацію. Відповідно застаріли або зіпсовані зовнішні носії, подальша експлуатація яких вже неможлива, повинні бути утилізовані методом, який гарантує, що не буде втрати даних і що конфіденційність і безпека цих даних не будуть порушені.

Необхідно дотримуватися наступних кроків:

- співробітник, який використовує зовнішні носії, зобов'язаний визначити застаріли чи зіпсовані зразків для утилізації;
- заборонено самостійне викидання або утилізація зовнішніх носіїв;
- всі застаріли чи зіпсовані зразки передаються для знищення до відповідального з ІБ. Відповідальний з ІБ забезпечує знищення зовнішніх носіїв, що підлягають утилізації.

Зазначені правила стосуються зовнішніх носіїв, що є власністю Комунального закладу «Бахмутський медичний фаховий коледж». Особисті зовнішні носії, що використовуються співробітниками коледжу для зберігання робочої чутливої інформації, у разі неможливості їх подальшого використання, знищуються самостійно, з дотриманням всіх вимог, що зазначені в даному пункті ПІБ. Співробітники несуть персональну відповідальність за розповсюдження або випадкових виток інформації, яку вони обробляють відповідно до свої посадових обов'язків.

10.2. Утилізація комп’ютерного обладнання

Комп’ютерне обладнання, що належить Комунальному закладу «Бахмутський медичний фаховий коледж», яке підлягає утилізації, проходить відповідну процедуру, що складається з видалення усіх даних, затирання усіх міток та конфігурацій та повернення до заводських налаштувань. Відповідальний з інформаційної безпеки забезпечує утилізацію комп’ютерного обладнання відповідно до встановленої процедури.

10.3. Використання надлишкого обладнання

Оскільки старе комп'ютерне обладнання поступово замінюється більш сучасними цифровими системами, воно підлягає інвентаризації та зберіганню. Старе комп'ютерне обладнання може бути використане:

- для запасних частин;
- для аварійної заміни;
- для тестування нового програмного забезпечення;
- для створення та зберігання резервних копій для іншого виробничого обладнання;
- для використання співробітниками за межами закладу, в тому числі для забезпечення дистанційної роботи.

11. УПРАВЛІННЯ ЗМІНАМИ

Для того, щоб відстежувати та управляти змінами в мережах, IT-системах та на робочих станціях, включаючи встановлення та налаштування нового програмного забезпечення та виправлення вразливостей програмного забезпечення в інформаційних системах, які містять конфіденційну, фінансову або господарську інформацію, в Комунальному закладі «Бахмутський медичний фаховий коледж» запроваджена процедура управління змінами, яка полягає в наступному:

1. Інженер-програміст або інший призначений працівник, який здійснює оновлення, встановлення, перелаштовує або іншим чином вносить зміни у мережеве та комп’ютерне обладнання, повинен ретельно реєструвати всі зміни, які проводяться у журналі обліку обладнання та програмного забезпечення, та також в картках робочої станції.
2. Інженер-програміст або працівник, який впроваджує зміну, забезпечує створення всіх необхідних резервних копій програмного забезпечення та даних.
3. Працівник, який впроваджує зміну, також повинен бути ознайомлений з процесом повернення до попередніх налаштувань у тому випадку, якщо зміна викликає збоїв в мережі чи системах і потребує видалення.

В Комунальному закладі «Бахмутський медичний фаховий коледж» дозволене до використання тільки ліцензійне програмне забезпечення, та дозволене програмне забезпечення (Додаток 3). Оновлення ліцензійного та дозволеного програмного забезпечення проводиться відповідно до рекомендацій

розробників цього ПЗ. Персонал повинен здійснювати оновлення програмного забезпечення невідкладно, по мірі отримання/можливості доступу до оновленої версії ПЗ.

Під час дистанційної роботи та використанні особистих пристроїв співробітників для обробки інформації, що стосується діяльності Комунального закладу «Бахмутський медичний фаховий коледж», дотримання вищевказаних правил обов’язкове. Використання неліцензованого програмного забезпечення на комп’ютерах, де обробляється чи зберігається інформація, яка стосується діяльності коледжу – неприпустиме.

12. МОНІТОРИНГ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В Комунальному закладі «Бахмутський медичний фаховий коледж» запроваджені програмні засоби моніторингу інформаційної безпеки, які входять до складу антивірусного програмного забезпечення та журналювання операційної системи.

Моніторинг стану інформаційної безпеки – це відповідні технологічні та процесуальні дії, які спрямовані на відстеження і фіксацію комп'ютерної та мережевої діяльності з метою визначення, чи сталося порушення інформаційної безпеки. Моніторинг передбачає відстеження та фіксацію зареєстрованих комп'ютерних подій, які стосуються стану операційних систем, програмного забезпечення або діяльності користувачів.

В закладі проводиться моніторинг діяльності користувачів з метою запобігання технологічних збоїв та виявлення потенційних ризиків та вразливостей системи інформаційної безпеки. Відповідно до виявлених збоїв, ризиків та вразливостей в закладі розробляються та запроваджуються відповідні адміністративні, фізичні та технічні заходи забезпечення інформаційної безпеки відповідно до вимог чинного законодавства у сфері інформаційної безпеки. Процедура моніторингу полягає у наступному:

1. Весь персонал та керівництво ознайомлене з чинною політикою інформаційної безпеки та дотримується її положень при виконанні службових обов’язків.
2. Інженер-програміст забезпечують моніторинг та обробку журналів подій на всіх комп'ютерних системах, що містять та/або обробляють чи

зберігають конфіденційну інформацію та персональні дані. Моніторинг, як мінімум, повинен включати: визначення ідентифікатора користувача, час і дату входу, а також обсяг та характер даних, до яких був отриманий доступ або спроба доступу.

В закладі використовуються програми антивірусного захисту, а також брандмауери, що фіксують події, пов’язані із можливим атаками, збоями та діяльністю шкідливого програмного забезпечення. Відповідальний з інформаційної безпеки організовує та забезпечує встановлення, обслуговування та оновлення таких систем.

Комунальний заклад «Бахмутський медичний фаховий коледж» Політика інформаційної безпеки	
Назва: АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	Розділ 13
Дата затвердження 30.05.2024 Дата набрання чинності: 01.06.2024	Огляд: Щорічний Інформаційна безпека закладів освіти; Інформаційна безпека закладів охорони здоров'я

13. АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В КЗ «Бахмутський медичний фаховий коледж» періодично, раз на рік, проводиться аудит стану інформаційної безпеки, який включає, але не обмежується такими заходами як, перевірка облікових записів користувачів та прав доступ до систем та мереж, доступ до файлів, перегляд та аналіз інцидентів безпеки, перегляд журналів моніторингу тощо. Аудит проводиться відповідним персоналом закладу. Мета проведення аудиту – мінімізація порушень безпеки та забезпечення інформаційної безпеки закладу на належному рівні. У разі неможливості проведення аудиту стану інформаційної безпеки власними силами та засобами, заклад може звернутись до авторизованих зовнішніх аудиторів. Процедура аудиту передбачає:

1. Ознайомлення аудиторів з політикою інформаційної безпеки, іншою документацією стосовно ІБ.
2. Інженер-програміст несе відповідальність за проведення періодичних оглядів діяльності інформаційних та мережевих систем та повинен мати відповідні технічні навички щодо безпечного застосування операційних систем, програмного забезпечення, додатків, баз даних, мережевого та медичного обладнання. Вказана особа надає доступ аудиторам до відповідних даних.
3. Відповідальний за ІБ повинен розробити формат звіту щодо результатів аудиту стану інформаційної безпеки та план усунення виявлених недоліків при необхідності. У такому звіті повинні бути вказані: хто проводив аудит, дата і час виконання, а також висновки, щодо стану

інформаційної безпеки закладу, виявлені недоліки та вразливості. До звіту можуть додаватися рекомендації аудиторів щодо підвищення рівня ІБ закладу, усунення вразливостей та мінімізації ризиків.

4. Аудит стану ІБ проводиться щорічно але може проводитися позапланова, якщо є підстави підозрювати порушення, які можуть призвести до тяжких наслідків. При проведенні перегляду журналів подій аудитори повинні перевірити наступне:

- логи подій - стосується вдалих/невдалих спроб входу, при цьому особлива увага приділяється саме невдалим спробам входу, блокуванням облікових записів та несанкціонованим спробам доступу;
- доступ до файлів – вдалі/невдалі спроби доступу до файлів, особлива увага невдалим спробам доступу, несанкціонованому доступу і несанкціонованим спробам створення, зміни або видалення файлів;
- інциденти безпеки – перевіряються записи з журналу виявлення інцидентів безпеки та журналів моніторингу стану систем на предмет аномальних чи підозрілих дій або подій зі шкідливою логікою (наприклад, дій вірусів, хробаків, шкідливих експлойтів), відмовою в обслуговуванні або спробами сканування, тощо;
- облікові записи користувачів – перегляд облікових записів користувачів у всіх системах з метою переконатися, що користувачі не мають надлишкових прав доступу до інформаційних системах, та надлишкових прав поводження з інформацією;
- дати отримання ЕЦП і КЕП для систем, де вони застосовуються;
- умови зберігання фізичних носіїв ідентифікації користувачів.

Усі важливі висновки повинні бути відображені у звіті щодо аудиту стану інформаційної безпеки закладу. Особи що проводили аудит передають звіт та перелік рекомендованих заходів відповідальному з інформаційної безпеки для ознайомлення та вживання відповідних заходів. Відповідальний з ІБ при отримані звіту повинен невідкладно вжити всіх належних заходів з приведення стану ІБ до відповідного рівня та усунення виявлених недоліків.

Комунальний заклад «Бахмутський медичний фаховий коледж» Політика інформаційної безпеки	
Назва: ЦІЛІСНІСТЬ ДАНИХ ЗДОБУВАЧІВ ОСВІТИ	Розділ 14
Дата затвердження 30.05.2024 Дата набрання чинності: 01.06.2024	Огляд: Щорічний Інформаційна безпека закладів освіти; Інформаційна безпека закладів охорони здоров’я

14. ЦІЛІСНІСТЬ ДАНИХ ЗДОБУВАЧІВ ОСВІТИ

Комунальний заклад «Бахмутський медичний фаховий коледж» впроваджує та підтримує відповідні організаційні та технологічні заходи для підтвердження того, що особисті данні та інша конфіденційна інформація стосовно студентів – не були змінені або знищені несанкціонованим чином. Метою таких дій є забезпечення цілісності даних здобувачів освіти.

Заклад підтримує впровадження автоматизованих систем та програмного забезпечення, для автоматичної перевірки наявності людських помилок при обробці даних студентів. Відповідно до Закону України «Про освіту» та , обробка даних студентів здебільшого здійснюється через систему ЄДЕБО, яка має інструменти, що покликані мінімізувати можливості втрати чи оприлюднення даних добувачів освіти.

Єдина державна електронна база з питань освіти представляє собою інтегровану інформаційно-телекомунікаційну систему, технічні засоби якої перебувають в межах території України, складається з комплексу автоматизованих робочих місць, об’єднаних в єдину інформаційну систему засобами зв’язку з використанням технології віддаленого доступу, має підключення до мереж зв’язку загального користування з розмежуванням прав доступу, забезпечує захист від порушень цілісності інформації, забезпечує різні рівні доступності відкритої інформації та інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом

Щоб забезпечити цілісність даних, у разі необхідності їх передачі, застосовується шифрування даних що передаються. Також для забезпечення

цілісності даних студентів використовується шифрування при зберіганні таких даних.

Коледж забезпечує перевірку можливого дублювання даних у своїх комп'ютерних системах та мережах, щоб запобігти поганій інтеграції даних між різними комп'ютерними системами.

Для запобігання збою систем, які можуть призвести до порушення цілісності даних, заклад освіти забезпечує перевірку своїх інформаційні системи на точність і функціональність, перш ніж почне їх використовувати. ІТ-системи та мережеве обладнання проходить оновлення при випуску виробниками виправлень та оновлених версій програмного та апаратного забезпечення, які усувають виявлені помилки та недоліки.

Заклад встановлює та регулярно оновлює антивірусне програмне забезпечення на всіх робочих станціях, щоб своєчасно виявити та запобігти зміні або знищенню даних шкідливим програмним забезпеченням.

15. ПЛАНИ РЕЗЕРВНОГО КОПІЮВАННЯ ТА АВАРІЙНОГО ВІДНОВЛЕННЯ

В Комунальному закладі «Бахмутський медичний фаховий коледж» проваджені заходи та процедури реагування на надзвичайні події, які можуть завдати шкоди комп'ютерним системам та мережам, а також інформації – даним, що зберігаються локально на робочих станціях. Для цього розроблений План аварійного відновлення та План резервного копіювання. Коледж періодично (один раз на рік) переглядає цій план з метою аналізу його ефективності та оцінки ризиків для внесення відповідних корегувань.

15.1. План резервного копіювання

Відповідальний з ІБ забезпечує розробку та впровадження плану резервного копіювання даних для створення та підтримки точних копій операційних систем, програмного забезпечення, баз даних, іншої інформації та даних закладу. План передбачає заходи з резервного копіювання даних, зберігання та відновлення даних з резервних копій. Також План повинен передбачати наступні положення:

1. Резервне копіювання здійснюється за індивідуальними особливостями даних, що потрібно зберігати. Резервні копії операційних систем створюються раз на тиждень автоматично, після відповідних налаштувань кожної робочої станції. Резервні копії чутливої інформації робляться щонайменше раз на тиждень і зберігаються на з'ємних

носіях. Інформація, яка не є конфіденційною додатково копіюється на хмарні сервіси. Використання хмарних сервісів для резервного копіювання конфіденційної інформації, або інформації, що стосується фінансової чи господарської діяльності, на хмарні сервіси – заборонено. Резервні носії, які більше не експлуатуються, утилізуються відповідно до процедури «Утилізація зовнішніх носіїв».

2. Відповідальний за ІБ стежить за зберіганням і своєчасним видаленням резервних копій і забезпечує дотримання всіх належних заходів контролю доступу.
3. Відповідальний за інформаційну безпеку забезпечує щорічне тестування процедури резервного копіювання, щоб переконатися, що резервні копії створені та доступні.

У разі дистанційної роботи з чутливою інформацією, відповідальний за інформаційну безпеку розробляє індивідуальні вказівки щодо резервного копіювання інформації для кожного окремого випадка. Співробітники, що працюють дистанційно несуть відповідальність за дотриманні вимог щодо резервного копіювання даних.

15.2. План аварійного відновлення

Відповідальний за ІБ розробляє та регулярно оновлює План аварійного відновлення з метою своєчасного відновлення та/або запобігання будь-яких втрат даних, систем, необхідних для забезпечення функціонування коледжу, господарської діяльності та надання якісних освітніх послуг. План аварійного відновлення має достатній рівень деталізації та необхідні пояснення, для того, щоб він міг бути виконаний персоналом заходу в разі надзвичайної події.

План аварійного відновлення повинен містити наступне:

1. Порядок створення та оновлення копій документів щодо результатів інвентаризації інформаційних активів та конфігурації мереж та робочих станцій;
2. Паперову копію Плану резервного копіювання;

3. Список групи реагування у надзвичайних ситуаціях, члени якої несуть відповідальність за:
    - визначення впливу надзвичайної ситуації на заклад;
    - визначення безпечного місця розташування закладу;
    - порядок відновлення втрачених даних;
    - порядок використання аварійних систем протягом часу коли основні інформаційні системи недоступні;
    - необхідні заходи для відновлення функціонування закладу.
4. Процедуру реагування на втрату електронних даних, включає, але не обмежуючись, пошуком і завантаженням даних з найбільш актуальної резервної копії.
5. Номери телефонів та/або адреси електронної пошти всіх осіб, з якими потрібно зв'язатися у разі надзвичайної ситуації, у тому числі: членів групи реагування; осіб, які відповідають за зберігання та відновлення резервних даних.
6. Група реагування повинна збиратися щорічно, щоб:
    - переглянути План аварійного відновлення;
    - запланувати проведення навчань стосовно дій у надзвичайних ситуаціях та оцінити результати таких навчань;
    - переглянути паперові версії Плану резервного копіювання та Плану аварійного відновлення та зробити у них відповідні зміни.

Відповідальний за ІБ надає пропозиції щодо внесення змін до планів резервного копіювання та аварійного відновлення відповідно до результатів аналізу ризиків інформаційної безпеки. В Комунальному закладі «Бахмутський медичний фаховий коледж» до групи реагування входять:

- Красножон Наталя – директор;
- Воронцова Олеся – начальник кадрової служби;
- Завражна Ганна – адміністратор ЄДЕБО;
- Кірпа Юлія – головний бухгалтер.

16. ОБІЗНАНІСТЬ ТА НАВЧАННЯ З ПИТАНЬ БЕЗПЕКИ

Для підвищення обізнаності стосовно питань інформаційної безпеки всі співробітники Комунального закладу «Бахмутський медичний фаховий коледж», які працюють з конфіденційною або чутливою інформацією, обчислювальною технікою, що має доступ до внутрішніх баз даних коледжу чи on-line сервісів, включаючи керівництво, повинні регулярно проходити відповідні навчання. Навчання з ІБ для всього персоналу проводиться раз на рік, або позапланово при необхідності.

Навчальна програма з інформаційної безпеки. Відповідальний за інформаційну безпеку організовує та проводить навчання з інформаційної безпеки. Він здійснює первинний інструктаж для нових працівників, щорічний інструктажі для всього персоналу, а також планові заняття стосовно Політики інформаційної безпеки та актуальних загроз. Для проведення навчань, відповідальний з ІБ може залучати інших працівників та сторонніх експертів, в тому числі розробників програмного забезпечення або надавачів відповідних сервісів. Відвідування або участь у такому навчанні є обов'язковим для всіх співробітників, що описані вище. Відповідальний за інформаційну безпеку веде відповідну документацію про всі навчальні заходи.

Відповідальний з ІБ, при необхідності, може організовувати позапланові навчання при змінах у апаратному або програмному забезпечені, збільшені загроз, внесені змін у політику інформаційної безпеки, за результатами аудиту, тощо.

Пам’ятка з інформаційної безпеки. Відповідальний за ІБ розробляє пам’ятку з інформаційної безпеки, до якої включає правила кібергігієни та

правила чистого столу. Пам’ятка містить актуальну інформацію стосовно безпеки паролів, шкідливого програмного забезпечення, ідентифікації та реагування на інциденти, а також контролю доступу. Відповідальний за ІБ забезпечує доведення пам’ятки з інформаційної безпеки до всього персоналу. Окрім того він може поширювати спеціальні повідомлення до персоналу стосовно нових загроз, небезпеки, вразливостей та необхідних заходах інформаційної безпеки.

Захист від шкідливого програмного забезпечення. У рамках вищезазначеної навчальної програми з безпеки відповідальний за ІБ проводить навчання щодо запобігання ураження та протидії шкідливому програмному забезпеченню. Таке навчання повинно включати в себе наступне:

- вказівки щодо поводження з підозрілим вкладенням електронної пошти, електронними листами від незнайомих відправників і шахрайських повідомлень;
- важливості оновлення антивірусного програмного забезпечення та правил перевірки робочої станції або інших пристроїв на встановлення актуального антивірусного захисту;
- про небезпеку завантаження файлів з невідомих або підозрілих джерел;
- про ознаки небезпечного шкідливого програмного забезпечення, яке може обійти антивірусний захист або загроз «нульового дня»;
- важливість регулярного резервного копіювання критично важливих даних і зберігання даних в безпечному місці;
- дотримання правил антивірусного захисту при дистанційній роботі;
- про шкоду, яку можуть заподіяти віруси, трояни, хробаки та інше шкідливе програмне забезпечення;
- правила дій, якщо виявлено шкідливе програмне забезпечення на робочій станції.

Дотримання парольної політики. У рамках вищезазначеної навчальної програми з безпеки та нагадувань про безпеку персоналу відповідальний за ІБ проводить навчання щодо дотримання парольної політики. Таке навчання

стосується правил призначення та зміни паролів, а саме:

- необхідність зміни паролів кожні 30 днів;
- користувач не може повторно використовувати останні 6 паролів;
- паролі повинні містити не менше восьми символів і містити літери латинського алфавіту (верхнього регістру), малі та великі літери, цифри та спеціальні символи;
- заборону вживання прізвищ, імен, дат днів народження або номерів телефонів для призначених паролів;
- негайній зміні паролю при його компрометації або розголошені;
- заборону передачі паролів іншим працівникам та стороннім особам, включаючи членів родини;
- заборону на запис паролів на папері, у робочому блокноті та іншому незахищеному місті біля робочої станції;
- заборону на завантаження, онлайн використання чи входу до стороннього програмного забезпечення та/або входу до web-сайтів з автоматичним завантаженням паролів під час наступного доступу до цих ресурсів;
- будь-який працівник, якому відповідальний з ІБ доручив змінити свій пароль, тому що призначений пароль не відповідав вищезазначеним стандартам, повинен зробити це негайно.

Особи, що входять до робочої групи з інформаційної безпеки коледжу проходять навчання в зовнішніх закладах з обов’язковим підтвердженням успішності курсів. Тематика і напрямки курсів визначаються на засіданні зазначеної групи.

17. УПРАВЛІННЯ РИЗИКАМИ

Для забезпечення інформаційної безпеки Комунальний заклад «Бахмутський медичний фаховий коледж» проводить точну та ретельну оцінку потенційних ризиків та вразливостей стосовно конфіденційності, цілісності та доступності даних, що зберігаються, обробляються та передаються інформаційними системами та мережами закладу.

Заклад проводить точний і ретельний аналіз ризиків, результат цього аналізу служить основою для організації зусиль із забезпечення інформаційної безпеки закладу на належному рівні. Заклад проводить повторну оцінку ризиків безпеки та оцінку ефективності заходів безпеки, якщо це необхідно при змінах у штатній структурі, створені нових процесів чи розвитку технологій.

Процедура. ВІБ організовує та координує аналіз та оцінку ризиків. Для цього він залучає відповідних осіб з числа співробітників коледжу. Аналіз ризиків повинен відбуватися таким чином:

1. Проводиться інвентаризація та аналіз наявних інформаційних системи.

- оновлюється або здійснюється інвентаризації інформаційних систем: складається перелік всього інформаційного обладнання (наприклад, мережевих пристроїв, робочих станцій, принтерів, сканерів, мобільних пристроїв) і програмного забезпечення (наприклад, операційних систем, додатків, іншого програмного забезпечення та інтерфейсів); в переліку вказується: назва інформаційної системи, дата придбання, місцезнаходження, постачальник, ліцензії, графік технічного обслуговування та функції; здійснюється оновлення або розробка

мережевої архітектури.

- Оновлюється або розробляється макет об'єкта, що показує розташування обладнання всіх інформаційних систем, джерел живлення, телефонних роз'ємів; та іншого телекомунікаційного обладнання, мережевих точок доступу, схеми пожежної та охоронної сигналізації та обладнання, а також місця зберігання небезпечних матеріалів;
- для кожного елементу макету об’єкта ідентифікується відповідальний (авторизований користувач), вказується його посада та спосіб отримання дозволу на авторизоване користування;
- Для кожної інформаційної системи вказується:
  - пов’язані дані, про які зазначається, чи створені дані закладом або отримані від третьої сторони (якщо дані отримані від третьої сторони, зазначається спосіб отримання);
  - чи зберігаються дані тільки всередині організації або передаються третій стороні (якщо дані передаються третій стороні, визначають цю сторону, а також мету і спосіб передачі);
  - критичність інформаційної системи для закладу та пов'язаних з нею даних. Критичність визначають як високу, середню або низьку. Критичність - це ступінь впливу на діяльність закладу інформаційної системи, уразі якщо пов'язані з нею дані стануть недоступними протягом певного періоду часу;
  - визначена чутливість даних як висока, середня або низька. Чутливість - це характер даних пов’язаний з оцінкою шкоди, яка може виникнути в результаті порушення конфіденційності даних;
  - визначені засоби контролю безпеки для кожного ідентифікованого програмного забезпечення, що застосовується в інформаційних системах, із зазначенням процедури контролю та засобів контролю.
- При оцінці загроз конфіденційності, цілісності та доступності даних, які створених, отримані, зберігаються, передаються чи обробляються закладом звертається увага на таке:

- загрози пошкодження даних навколишнім середовищем, наприклад, землетрусом, повінню, штормом, тощо;
- загрози надзвичайних ситуацій - пошкодження пожежею, аварією електромережі, припиненням отримання комунальних послуг, тощо;
- Людські загрози, а саме:
    - ♦ ненавмисні дії, наприклад, помилки при введені даних, використання несправного програмного забезпечення, нездатність оновити програмне забезпечення, відсутність належних фінансових та людських ресурсів для підтримки необхідних засобів контролю безпеки;
    - ♦ неналежна діяльність, наприклад, неналежна поведінка, зловживання привілеями чи правами, марнотратство, переслідування особистої користі;
    - ♦ зловмисні дії, наприклад шахрайство, крадіжки, вандалізм, диверсії,
    - ♦ зовнішні атаки, наприклад, хакерські атаки, сканування, геополітичні ризики.

2. Виявляються вразливості інформаційних систем. Вразливість - це недолік або слабкість у процедурах безпеки, розробці, впровадженні або контролі за використанням ІС, які можуть бути випадково спровоковані або навмисно використані, що призведе до несанкціонованого доступу, модифікації даних, відмові в обслуговуванні або відмові від ідентифікації (неможливості ідентифікувати джерело зловмисних дій і притягнути якусь особу до відповідальності за ці дії). Для виконання цього завдання проводиться аналіз стосовно використання та застосування стандартів інформаційної безпеки до конкретних ІС і визначається ймовірність інциденту безпеки через вразливість інформаційної системи. Ймовірність інциденту безпеки визначається як:

- «Дуже ймовірно» - такий, що має дуже високі шанси на виникнення;
- «Ймовірно» - такий, що має значний шанс на виникнення;

- «Мало ймовірно» - незначний шанс на виникнення.

3. Одночасно визначається рівень критичності для вразливості інформаційної системи, як:

- «Високий» - такий, що має катастрофічний вплив на освітню діяльність закладу, призведе до втрати чи компрометації значної кількості фінансових даних або персональних даних здобувачів освіти;
- «Середній» - такий, що має значний вплив на діяльність закладу освіти, може призвести до втрати або компрометації персональних даних здобувачів освіти;
- «Низький» - визначається як незначний вплив, включаючи незначну втрату або компрометацію деяких даних щодо діяльності коледжу.

4. Визначається показник ризику для кожної вразливості шляхом компіляції оцінок ймовірності та критичності. Ризики з більш високим показником ймовірності та критичності вимагають більшої уваги.
5. Визначаються відповідні заходи безпеки для усунення або мінімізації ризиків. Основні зусилля зосереджуються на усунені вразливостей з високими показниками ризику. Ризики які неможливо усунути чи мінімізувати приймаються. Це означає, що керівництво йде на такий ризик та усвідомлює наслідки.
6. Розробляється або уточняється політика інформаційної безпеки та здійснюються конкретні критично важливих заходів безпеки (наприклад закупівля відповідної системи інформаційної безпеки або зміна програмного забезпечення на більш функціональне), а саме:

- визначається термін реалізації;
- визначити витрати на такий захід та джерело фінансування;
- призначається відповідальна особа;
- визначається порядок здійснення заходу;
- термін завершення;
- робиться попередня оцінка ефективності заходу, яка після здійснення уточняється.

7. Відповідальний за ІБ здійснює оцінку ефективності заходу стосовно усунення чи мінімізації ризику та при необхідності забезпечує здійснення повторної оцінки, яка включає:

- огляд користувачів з метою аналізу ефективності заходу, перегляд процедур, планів та політики інформаційної безпеки, аналіз інцидентів безпеки, уточнення програми навчань з ІБ, тощо;
- для здійснення оцінки відповідальний може залучати відповідних працівників закладу.

Необхідно усвідомлювати, що під час дистанційної роботи закладу освіти, необхідно корегувати процедуру оцінки ризиків. До процедури може включатись:

- оцінка стороннього програмного забезпечення, що використовується на особистих комп'ютерах співробітників, які задіяні в організації освітнього процесу та господарської діяльності коледжу;
- оцінка каналів доступу до мережі Internet, які використовуються співробітники, що працюють віддалено;
- аналіз обсягів посадових обов'язків, що пов'язані з обробкою чутливої інформації;
- впровадження інструментів резервування обов'язків. Резервування обов'язків – процес, коли певні види робіт з обробки інформації, може виконувати не лише одна особа в межах закладу. Таким чином, у разі звільнення, лікарняного (або інших подій невідворотної сили) певного співробітника – не призведе до припинення процесів, що пов'язані з діяльністю коледжу і передбачають обробку інформації.

18. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ

Співробітники та адміністрація Комунального закладу «Бахмутський медичний фаховий коледж» повинні постійно захищати конфіденційність, цілісність та доступність інформації та забезпечувати підтримку інформаційної безпеки закладу на належному рівні. При порушенні чинного законодавства та політики інформаційної безпеки настає відповідальність за порушення.

До конфіденційної інформації закладу відноситься:

- персональні данні здобувачів освіти – індивідуальна інформація про студентів, яка знаходиться в будь-якій формі (електронна, паперова, усна);
- електронна персональна інформація - індивідуальна інформація здобувачів освіти, що вноситься до ЄДЕБО;
- інформацію про стипендію здобувачів освіти;
- інформація про співробітників та викладачів коледжу - будь-яка інформація, пов'язана з наймам або працевлаштуванням будь-якої фізичної особи, яка є або була працевлаштована в коледжі;
- дані про заробітну плату співробітників та викладачів;
- фінансові/бухгалтерські записи - будь-які записи, пов'язані з бухгалтерською або фінансовою звітністю закладу;
- інша конфіденційна інформація – будь-яка інша інформація, яка має конфіденційний характер або вважається конфіденційною відповідно до чинних угод та договорів.

Терміни доступність, цілісність та конфіденційність вживаються відповідно до визначень, що наведені у п. 1.2. цієї політики.

Перелік порушень та відповідальність за них

Нижче перераховані види порушень, які вимагають застосування покарань. Вони діляться на три рівня перший (1), другий (2) і третій (3) в залежності від серйозності порушення та їх наслідків.

Рівень	Опис порушення
Перший рівень порушень (1)	- доступ до інформації, яка не потрібна для виконання службових обов'язків; - передача іншій особі персонального логіну та паролю та/або надання спільного доступу до робочої станції, авторизованого доступу; - залишення працюючого комп'ютера з доступом до конфіденційної інформації без нагляду; - розкриття конфіденційної інформації стороннім особам; - копіювання конфіденційної інформації без дозволу; - зміна конфіденційної інформації без дозволу; - обговорення конфіденційної інформації в публічному місці, де стороні особи мають можливість підслуховувати розмову; - обговорення конфіденційної інформації з неуповноваженою особою; - відмова від співпраці з відповідальним за ІБ та невиконання його вказівок щодо дотримання політики інформаційної безпеки.
Другий рівень порушень (2)	- здійснення порушення першого рівня вдруге (не обов'язково має бути тим самим порушенням); - несанкціоноване використання або розголошення конфіденційної інформації; - отримання доступу під логіном та паролем іншої людини; - невиконання/відмова у виконанні вказівок щодо виправлення ситуації.

Третій рівень порушень (3)	- здійснення порушення першого рівня втретє (не обов'язково має бути тим самим порушенням); - здійснення порушення другого рівня вдруге (не обов'язково має бути тим самим порушенням); - отримання конфіденційної інформації під вигаданими приводами; - використання та/або розкриття конфіденційної інформації з метою отримання особистої вигоди або здійснення зловмисних дій.

Дисциплінарні стягнення

У тому випадку, якщо працівник здійснив будь-яке з наведених вищі порушень до нього застосовуються наступні заходи дисциплінарного впливу чи покарання.

Рівень порушення	Дисциплінарні стягнення
Перший рівень порушень (1)	- усна або письмова догана; - або пониження прав доступу; - або направлення на додаткове заняття з інформаційної безпеки; - або проходження додаткового інструктажу з інформаційної безпеки
Другий рівень порушень (2)	- сувора догана із занесенням в особову справу; - або тимчасове відсторонення від виконання службових обов’язків; - або пониження прав доступу до рівня, що призводить до пониження у посаді чи рівні кваліфікації;; - або призначення проходження позапланового навчання (курсу навчань) в неробочій час;
Третій рівень порушень (3)	- припинення трудової діяльності або розірвання контракту; - та/або накладання штрафу для компенсації

	нанесених збитків; - та/або кримінальне покарання відповідно до чинного законодавства.

Дисциплінарні покарання носять виховуючи характер та застосовуються відповідно до певних обставин здійснення порушень. Адміністрація закладу проводить консультації з відділом кадрів та юристом перед вжиттям відповідних заходів. У відповідних випадках накладаються більш м'які дисциплінарні покарання, якщо порушник усвідомлює неправильність вчинку та налаштований скорегувати поведінку.

Накладання сурової догани повинно бути попередньо обговорено керівництвом з відділом кадрів та юристом коледжу.

В залежності від тяжкості наслідків порушення, будь-які окремі порушення першого та другого рівня можуть призвести до припинення трудової діяльності або розривання контракту з порушником.

Визнання відповідальності за порушення

Співробітники Комунального закладу «Бахмутський медичний фаховий коледж», що працюють з чутливою та конфіденційною інформацією повинні усвідомлювати про можливу відповідальність за порушення засад ІБ коледжу. Для фіксації цього використовується відповідна форма:

Я, нижче підписаний співробітник, цим підтверджую отримання та ознайомлення з інформацією Комунального закладу «Бахмутський медичний фаховий коледж» стосовно відповідальності за порушення інформаційної безпеки.

Дата *Підпис співробітника*

19. ПЕРЕВІРКА КАНДИДАТІВ

Комунальний заклад «Бахмутський медичний фаховий коледж» проводить довідкові перевірки кандидатів перед працевлаштуванням. Від кандидата завчасно отримується згода на проведення такої перевірки. Кандидат, який відмовляється від такої перевірки, перестає бути кандидатом та його вивчення кадровим відділом припиняється.

Відділ кадрів збирає інформацію про репутацію кандидата, особисті характеристики або спосіб життя. Ця інформація може бути зібрана в Internet, включаючи сайти соціальних мереж, через публічні чи освітні записи або через співбесіди з попередніми роботодавцями, особами, що можуть надати рекомендаційні листи або будь кім іншим.

Тип інформації, яка буде зібрана закладом під час перевірки біографічних даних, може включати, але не обмежуватися наступною інформацією:

- довідка про непритягувана до кримінальної відповідальності;
- диплом про освіту (включаючи середній бал);
- історію працевлаштування, здібності та причини припинення трудових відносин;
- відомості про здійснення підприємницької діяльності;
- сертифікати, дипломи про закінчення закладів навчання, курсів, тощо;
- кредитна історія;
- реєстр рішень цивільних судів;
- записи у відкритих реєстрах стосовно володіння рухомим та нерухомим майном;

- професійні або особисті довідки;
- резюме кандидата.

Ця інформація також може бути додатково переглянута під час здійснення працівником порушення або його/її перепризначення на посаду з розширенням прав доступу. Повідомлення про судимість не обов'язково дискваліфікує кандидата на працевлаштування. При прийняті рішення враховується характер і серйозність правопорушення, дата правопорушення, обставини та можливі ризики для закладу при працевлаштуванні такого кандидата.

Коледж має право відкликати пропозицію про працевлаштування, або звільнити працівника при виявлені свідомого надання неправдивої інформації стосовно себе.

Звіти про перевірку біографічних даних зберігається, як конфіденційна інформація відділом кадрів.

Комунальний заклад «Бахмутський медичний фаховий коледж» Політика інформаційної безпеки	
Назва: РЕАГУВАННЯ НА ІНЦИДЕНТ	Розділ 20
Дата затвердження 30.05.2024 Дата набрання чинності: 01.06.2024	Огляд: Щорічний Інформаційна безпека закладів освіти; Інформаційна безпека закладів охорони здоров'я

20. РЕАГУВАННЯ НА ІНЦИДЕНТ

Повідомлення про порушення

1. Будь-який співробітник, викладач чи здобувач освіти, якому стало відомо про порушення політик інформаційної безпеки або про інцидент ІБ – негайно повідомляє про це директора коледжу та/або відповідального за ІБ.
2. Повідомлення повинно відбуватися негайно після виявлення можливого порушення.
3. Директор коледжу або відповідальний за ІБ перевіряє обставини можливого порушення та невідкладно вживає можливі заходи реагування на порушення.
4. Для негайного повідомлення про порушення або загрозу інформаційній безпеці коледжу необхідно зателефонувати відповідальному за інформаційну безпеку за номером телефону +380506319313.

Реагування на інцидент

Відповідальний за інформаційну безпеку при отримані повідомлення про порушення або інцидент самостійно або із залученням відповідних працівників коледжу вживає наступні заходи, з метою обмеження наслідків порушення чи інциденту:

1. Вживає заходів по збиранню та збереженню доказів та припиняє несанкціоновану дію.
2. Відключає або локалізує інформаційну систему, яка може бути уражена.
3. По можливості відновлює записи, дані, що могли постраждати.

4. По можливості усуває вразливості та слабкі місця, які призвели до інциденту.
5. За рішенням керівника повідомляє правоохоронним органам (Національна поліція, кіберполіція) про інцидент безпеки та його ознаки.
6. Інформує Міністерство совіти і науки України та Міністерство охорони здоров'я України про значні інциденти інформаційної безпеки.

Розслідування та мінімізація ризиків

При інциденті інформаційної безпеки, що може причинити значні негативні наслідки відповідальний за ІБ долучає до розслідування членам Робочої групи з інформаційної безпеки.

1. Група розглядає обставини, причини та наслідки інциденту та оцінює ризики інформаційної безпеки, які пов'язані з інцидентом. При цьому розглядаються наступні фактори, але не обмежуються ними:

- характер цифрового активу, який постраждав в наслідок інциденту та його важливість для функціонування закладу;
- необхідні заходи та засоби для відновлення функціонування;
- договірні зобов'язання, які можуть бути не виконані, порушені;
- ризики крадіжки особистих даних або втрати інформації в наслідок її псування, затирання чи шифрування, можливості щодо відновлення якомога актуальнішої версії резервного копіювання;
- ризик заподіяння фізичної шкоди, якщо втрата даних ставить під загрозу життя людини;
- ризик заподіяння шкоди репутації закладу освіти;
- обсяги (масив) втраченої, вкраденої чи зіпсованої інформації та кількість постраждалих осіб.

Повідомлення постраждалих

1. Відповідно до чинного законодавства заклад повідомляє постраждалим особам про виток їх персональних даних.
2. Постраждалі особи повинні бути повідомлені не пізніше двох місяців після відбуття інциденту. Повідомлення повинні містити наступну інформацію:

- що сталося;
- яка сама персональна інформація стосовно постраждалої особи вкрадена (скомпрометована) чи зіпсована;
- рекомендації, що постраждалій особі бажано зробити;
- інформація про дії коледжу для запобігання подібних інцидентів у майбутньому;
- контактна інформація.

Повідомлення надсилається на електронну пошту постраждалої особи або інший електронний акаунт.

3. Якщо заклад повідомив про інцидент правоохоронні органи то інформування постраждалих осіб відбувається тільки після дозволу правоохоронців, щоб не перешкоджати кримінальному розслідуванню.
4. Непряме сповіщення, таке як публікація інформації на веб-сайті або сторінці закладу у соціальних мережах, може відбутися коли кількість постраждалих значна.
5. Використання декількох методів оповіщення в певних випадках може виявитися найбільш ефективним підходом.

Профілактика

1. Після вжиття негайних заходів для зменшення ризиків, пов'язаних з порушенням, відповідальний за ІБ проводить розслідування причин порушення. При необхідності може проводитися аудит безпеки фізичних, організаційних і технологічних заходів. Це також може включати перегляд політики інформаційної безпеки.
2. Для проведення розслідування причин інциденту відповідальний за ІБ залучає відповідних працівників коледжу та при необхідності зовнішніх експертів.
3. Результати розслідування доповідаються директору коледжу разом з рекомендаціями, щодо запобігання подібних інцидентів у майбутньому.
4. За результатами складається план заходів з усунення недоліків, виявлених в ході розслідування інциденту, якщо це доречно.

Відповідальність

Керівник коледжу несе повну відповідальність за захист даних та підтримку належного рівня інформаційної безпеки закладу. Адміністрація та всі співробітники закладу, які порушують політику інформаційної безпеки та/або чинне законодавство несуть дисциплінарну, адміністративну чи кримінальну відповідальність.

Додаток 1

ФОРМА ЗАПИТУ НА ДОСТУП

(запит працівника чи підрядника на доступ до інформаційних ресурсів)

ПІБ

Посада

Дата початку доступу

Режим доступу (цілодобовий чи у певні робочі години)

Дата та час припинення доступу

Перелік ресурсів до яких надається доступ з вказанням прав доступу (читання, редагування даних, КЕП, відвідування у вихідні дні тощо).

1. Електронна пошта
2. Електронні реєстри
3. Внутрішні бази та зовнішні сервіси
4. Програмне забезпечення, додатки
5. Віддалений доступ
6. Службовий телефон
7. Доступ до будівлі

Погодження безпосереднього керівника

Погодження відповідального за ІБ

Додаток 2

Згода про нерозголошення

ВІДПОВІДАЛЬНІСТЬ ЗА РОЗГОЛОШЕННЯ
КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Я _____

розумію і погоджуюся зберігати, захищати та не розголошувати конфіденційну інформацію Комунального закладу «Бахмутський медичний фаховий коледж». Крім того, я розумію, що будь-яке несанкціоноване використання або розголошення інформації закладу, може призвести до дисциплінарної, адміністративної чи кримінальної відповідальності відповідно до політики інформаційної безпеки Комунального закладу «Бахмутський медичний фаховий коледж» та чинного законодавства.

Дата Підпис

Дата Підпис відповідального за ІБ