

**Положення БО «БФ «АДРА Україна» про систему контролю**

**та користування Інтернет мережею**

1. **Викладення головних положень**

А. В даних положеннях викладені правила, яких повинні притримуватися всі співробітники та ті, хто надають послуги (ЦПУ та ФОП) БО «БФ «АДРА Україна» при використанні комп'ютерів БО «БФ «АДРА Україна», смартфонів та іншого комп'ютерного обладнання, програмного забезпечення, облікових записів комп'ютерів або програм та інтернету з будь-якого комп'ютера БО «БФ «АДРА Україна», використовуючи всесвітню мережу (WWW) та внутрішні мережі БО «БФ «АДРА Україна» («Мережа БО «БФ «АДРА Україна»»).

Б. Дані положення поширюються на особисте використання системи електронної пошти БО «БФ «АДРА Україна». Більш того, співробітники, та ті, хто надають послуги (ЦПУ та ФОП), повинні відповідально ставитися до користування електронною поштою та притримуватися політики конфіденційності даних.

В. В даних положеннях пояснюються законні дії БО «БФ «АДРА Україна» в якості роботодавця стосовно контролю за використанням мереж та комп’ютерів БО «БФ «АДРА Україна» та проведення розслідування щодо порушень встановлених правил персоналом або третьою особою, що розлягається як неприпустима поведінка.

Г. Дані положення застосовуються до будь-якої особи, яка використовує мережі або комп’ютери БО «БФ «АДРА Україна» для доступу в інтернет та до електронної пошти. В даних положеннях термін "персонал" або "користувач" означає будь-яку особу, яка працює або надає послуги (ЦПУ та ФОП) в БО «БФ «АДРА Україна», або особу, яка не є штатним працівником, але працює на території, яка належить організації (наприклад: студенти, стажисти або волонтери), або будь-яку особу, яка працює, чи надає послуги (ЦПУ та ФОП) за контрактом в БО «БФ «АДРА Україна» (незалежний підрядник, консультант або тимчасовий співробітник). Всі дані категорії розглядаються, як "персонал БО «БФ «АДРА Україна»".

Д. Доступ до мереж БО «БФ «АДРА Україна» або інтернету надається в першу чергу персоналу БО «БФ «АДРА Україна» для ефективної роботи БО «БФ «АДРА Україна» та розвитку навичок та знань персоналу БО «БФ «АДРА Україна». Дозволяється обмежене особисте користування інтернет мережею.

Е. Інформація, яка доступна на мережах БО «БФ «АДРА Україна» або в інтернеті, пов'язана з певним ризиком щодо безпечності використання даної інформації, її цілісності, конфіденційності, контролю та притримування певних норм.

Є. Захист даних. Президент, або довірене лице БО «БФ «АДРА Україна» має право контролювати всі дії користувачів інтернету для цілей, зазначених у розділі IV.A. Інформація, яка необхідна для проведення контролю, включає наступне: ідентифікацію користувача, назви доменів відвіданих веб-сайтів, тривалість відвідувань та завантажені файли або файли, які знаходяться в процесі завантаження. Персонал повинен знати, що даний контроль може виявити особисті дані користувача, посилаючись на сайти, які він відвідував: політичну думку або релігійні переконання, стан психічного або фізичного здоров’я. Персонал, який користується інтернетом, повинен дати згоду на те, що БО «БФ «АДРА Україна» може обробляти їхню конфіденційну особисту інформацію під час проведення контролю. Якщо співробітники не погоджуються з даним положенням, то вони не повинні використовувати сайти БО «БФ «АДРА Україна» в особистих цілях. Таким чином, співробітники забезпечують конфіденційність особистих даних. З метою захисту даних БО «БФ «АДРА Україна» кожен співробітник, та той, хто надає послуги (ЦПУ та ФОП) організації, повинен при завершенні співпраці з БО «БФ «АДРА Україна» здати комп’ютер, телефон чи планшет (при наявності) та всю робочу інформацію у повному обсязі системному адміністратору. Забороняється видаляти будь-які файли, програми та інше. Усі файли особистого характеру дозволяється видалити тільки в присутності системного адміністратора.

1. **Мета**

Дані положення визначають стандарти для систем, які контролюються, та обмеження використання інтернет мереж з будь-якого комп'ютера БО «БФ «АДРА Україна». Дані положення розроблені для підтримки комп'ютерів та інтернет мереж у належному стані, для забезпечення конфіденційності, цілісності та надійності роботи мереж БО «БФ «АДРА Україна», для запобігання вторгнень в мережі БО «БФ «АДРА Україна» чи порушення конфіденційності особистих даних та для уникнення непередбачуваних обставин.

1. **Завдання**

Дані положення поширюються на всіх співробітників, підрядників, постачальників, користувачів, довірених осіб БО «БФ «АДРА Україна» та осіб, які користуються особистими чи державними комп’ютерами, підключеними до мереж БО «БФ «АДРА Україна». Дані положення поширюються на всіх користувачів, які використовують інтернет мережі БО «БФ «АДРА Україна», у тому числі веб-браузери, програми миттєвого обміну повідомленнями, системи передачі файлів, обмін файлами та інші протоколи користувачів.

В даних положеннях пояснюються законні дії БО «БФ «АДРА Україна» в якості роботодавця стосовно контролю за використанням мереж та комп’ютерів БО «БФ «АДРА Україна» та проведення розслідування щодо порушень встановлених правил персоналом або третьою особою, що розлягається як неприпустима поведінка.

1. **Стратегія**

А. Інтернет та поточний контроль мережі

1. БО «БФ «АДРА Україна» може час від часу перевіряти можливості вторгнення у свої мережі для того, щоб виявити несанкціоноване використання комп'ютерів БО «БФ «АДРА Україна», мереж організації або телекомунікаційних систем; попередити виникнення непередбачуваних ситуацій, порушень правил безпеки роботи з комп'ютерним обладнанням, правил користування та норм стандартного захисту комп’ютерів. Ці положення розроблені для того, щоб захистити дані БО «БФ «АДРА Україна» та особисті дані клієнтів організації, які зберігаються в мережах БО «БФ «АДРА Україна».

2. З метою збереження цілісності мережі організації та даних, які розташовані в даній мережі, БО «БФ «АДРА Україна» має право контролювати використання інтернету, мережевий трафік, а також використання всіх комп'ютерів та пристроїв БО «БФ «АДРА Україна», які підключені або не підключені до мережі БО «БФ «АДРА Україна».

3. Інформація, яка зберігається на системі автоматизованого контролю, може бути використана для ідентифікації окремого користувача та перегляду веб-сайтів та документів, якими він користувався, та визначення часу, витраченого на перегляд даних документів. Співробітники повинні знати, що перегляд будь-якої інформації в мережі БО «БФ «АДРА Україна» в неробочий час, також фіксується.

4. У разі виявлення порушень даних положень, необхідно повідомити про це керівників, юристів або співробітників БО «БФ «АДРА Україна», які слідкують за порядком. Організація БО «БФ «АДРА Україна» залишає за собою право здійснювати детальну перевірку, робити копії всіх документів, пристроїв та фотографій, що містять дані БО «БФ «АДРА Україна», при необхідності.

Б. Доступ до звітів щодо поточного контролю на сайтах

Керівники, юристи або співробітники БО «БФ «АДРА Україна», які слідкують за порядком, повинні мати доступ до всіх звітів та даних організації для швидкого реагування на будь-яке порушення системи безпеки.

В. Система фільтрації інтернет користування

1. Співробітники ("персонал БО «БФ «АДРА Україна»") не повинні пересилати, завантажувати, роздруковувати, відображати або поширювати наступний матеріал в мережах БО «БФ «АДРА Україна» чи на будь-яких об’єктах, які належать організації:

• зображення, інформацію або інші матеріали, які містять непристойний підтекст;

• неякісні зображення або матеріал образливого змісту;

• матеріал, який принижує гідність певної раси;

• шахрайські або інші матеріали, добуті незаконним шляхом;

• матеріали, які пропагують насильство, нетерпимість або прояв ненависті до інших;

• будь-який матеріал, який можна використати у непристойному контексті.

До даного списку також належить використання нецензурної лексики, перегляд порнографічних сайтів, публікація матеріалів, які дискримінують людину за ознаками статі, раси, сексуальної орієнтації, релігійних та політичних переконань, інвалідності; інформації, яка може сприяти виникненню ненависті, насильства або інформації, яка принижує людину, викликає роздратування, причиняє незручність та неспокій, суперечить основним положенням БО «БФ «АДРА Україна».

2. Персоналу БО «БФ «АДРА Україна» забороняється:

• навмисно порушувати механізми безпеки, зламувати паролі та незахищені системи, використовувати інформаційні системи понад наданих можливостей;

• навмисно писати, розробляти, копіювати або поширювати будь-яку комп'ютерну програму, яка може пошкодити операційній системі комп'ютера. До таких програм належать наступні шкідливі віруси: мікроб, програма-хробак або Троянський кінь.

• пересилати, завантажувати, розміщувати або обговорювати особисті дані, конфіденційну інформацію про стан здоров’я або особисті дані співробітників та тих, що надають послуги (ЦПУ та ФОП) БО «БФ «АДРА Україна» з будь-якою третьою стороною без попереднього письмового дозволу від керівництва БО «БФ «АДРА Україна».

• завантажувати файли та програми, без безпосереднього дозволу системного адміністратора (з метою захисту даних організації від проникнення вірусів в комп’ютер або в систему).

• на власний розсуд видаляти будь-які файли з робочого комп’ютера чи планшета (робочого та особистого характеру).

3. Крім перерахованого вище, інтернет доступ забороняється у наступних випадках:

• будь-яка діяльність, яка порушує авторські права;

• розповсюдження комерційного або рекламного матеріалу за власною ініціативою;

• незаконний доступ до об'єктів або послуг через інтернет;

• знищення даних іншого користувача;

• будь-яка діяльність, яка втручається в приватне життя інших співробітників;

• будь-яка діяльність, яка шкодить репутації БО «БФ «АДРА Україна»;

• пошкодження організаційних систем;

• будь-яка діяльність, пов’язана з порушенням законів та постанов України;

• використання інтернет мереж організації для іншої роботи за певну плату або безкоштовно;

• використання інтернет мереж організації для розвитку власної підприємницької діяльності.

4. БО «БФ «АДРА Україна» залишає за собою право блокувати доступ до інтернет-сайтів та документів, які не відповідають стандартам БО «БФ «АДРА Україна». Прикладами документів та сайтів, які можуть бути заблоковані, є наступні:

• порнографічні сайти;

• сайти зі спливаючими рекламними оголошеннями;

• сайти з азартними іграми;

• сайти з незаконною інформацією;

• сайти, де продаються незаконні наркотичні засоби;

• сайти з продажу нижньої білизни та купальників;

• сайти, де можна обмінюватися будь-якими файлами з іншими користувачами інтернету;

• сайти, з яких можна відправляти «спам» повідомлення для отримання конфіденційної інформації або брати участь в інших видах шахрайства;

• шпигунські сайти;

• сайти з матеріалами, які принижують гідність інших людей;

• сайти, які направлені на приниження гідності певних рас, сприяють прояву насильства, нетерпимості та ненависті до інших людей;

• соціальні мережі;

• сайти розважального характеру.

Д. Винятки щодо використання заборонених інтернет ресурсів

Після отримання письмового дозволу від керівництва організації щодо розблокування сайту, який потрібен для більш ефективної роботи організації, персоналу БО «БФ «АДРА Україна» надається можливість користуватися даним сайтом. Для отримання даного дозволу необхідно подати заявку керівнику, який має оцінити необхідність розблокування певного сайту. Всі заявки, перевірені керівниками, необхідно надіслати керівництву БО «БФ «АДРА Україна» у письмовій формі або по електронній пошті. Керівництво БО «БФ «АДРА Україна» повинно оцінити заявки та розглянути можливість розблокування певних сайтів.

1. **Виконання положень**

А. Співробітники, та ті, хто надають послуги (ЦПУ та ФОП) БО «БФ «АДРА Україна» зобов’язані повідомляти керівників БО «БФ «АДРА Україна» про можливі порушення даних положень.

Б. До співробітника, який порушив дані положення, можуть бути застосовані різні дисциплінарні стягнення, у тому числі звільнення.

1. **Визначення**

Сайти «хакерів» – це сайти, які містять інформацію щодо злому або пошкодження програм комп'ютерної безпеки.

Надзвичайна ситуація – це подія або ціла група подій, пов’язаних з системою безпеки, які призводять до порушення безпеки інформаційних технологій. До надзвичайних ситуацій також належать порушення положень безпеки інформаційних технологій або загрози пошкодження системних фондів організації. Нижче наведені лише деякі приклади надзвичайних ситуацій:

• порушення конфіденційності інформації;

• порушення цілісності інформації;

• порушення доступності системи;

• відмова в обслуговуванні;

• неправильне використання систем обслуговування або інформації.

*Інтернет* – це відкриті мережі електронних комунікацій, який з'єднують комп'ютерні мережі та комп'ютери по всьому світу.

*Фільтрація інтернету* – це використання технологій, які контролюють зв'язок між комп’ютерами в корпоративній мережі та блокують трафік, згідно заданим правилам.

*Виявлення вторгнень* – це процес контролю подій, які відбуваються в комп'ютерних системах або мережах, та аналіз ознак можливих непередбачених ситуацій (порушення або загроза порушень положень щодо безпеки комп'ютерних технологій, правил користування або стандартів безпеки інформаційних технологій).

*IP адреса*– це унікальна адреса мережі, яка присвоюється кожному пристрою для з’єднання з іншими пристроями в інтернет мережі.

*Обмін файлами між користувачами* – це служби та протоколи, які дозволяють інтернет-користувачам скачувати та обмінюватися файлами з іншими користувачами.

*Фішинг* – це отримання конфіденційної інформації обманним шляхом через інтернет.

*SMTP* – це спрощений протокол електронної пошти, який забезпечує швидкий обмін поштовими повідомленнями між серверами.

*Соціальні мереж*і – це інтернет-сайти, такі як Myspace, Facebook та інші, які дозволяють користувачам розміщувати різну інформацію, спілкуватися та взаємодіяти в інтернет-спільнотах.

*Спам* - це небажана інтернет-пошта.

*Ідентифікація користувача* – це ім'я користувача або інший ідентифікатор, який необхідний для входу в корпоративні мережі.

1. **Поправки**

Дані положення, час від часу, потрібно міняти та переглядати. Персоналу БО «БФ «АДРА Україна» повинні надаватися документи зі всіма поправками та змінами, якщо інше не зазначено у даних документах. Після отримання даних документів співробітники зобов’язані притримуватися оновлених положень.

1. **Примітка**

При порушенні цього положення кожен з співробітників та тих, хто надавав послуги за ЦПУ та ФОП може бути притягнений до відповідальності згідно чинного законодавства (**Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»**)

ПІБ співробітника: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Підпис Дата

**ЗАТВЕРДЖЕНО ОПІКУНСЬКОЮ РАДОЮ:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**