

ЗАТВЕРДЖЕНО

Наказ голови правління КС “Юніон
Вінниччина” Н-223 від 01.10.2020р.

Голова правління

Бочаров О.Г.

Примірний План

дій працівників КС “Юніон Вінниччина” на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій

1. При виявленні ознак несанкціонованого доступу до персональних даних осіб таких як: несанкціоноване отримання логінів і паролів, підбір паролів та ключів, працівник, який виявив дані ознаки, зобов’язаний негайно:
 - припинити обробку персональних даних;
 - повідомити безпосереднього керівника та відповідальну особу, що організує роботу, пов’язану із захистом персональних даних при їхній обробці у КС “Юніон Вінниччина” (далі – відповідальна особа);
 - змінити паролі доступу (за наявності технічної можливості);
2. При виявленні зараження програмного забезпечення та носіїв інформації комп’ютерними вірусами працівник зобов’язаний:
 - негайно припинити обробку персональних даних;
 - вимкнути комп’ютерну техніку від електроживлення;
 - повідомити безпосереднього керівника та відповідальну особу.
3. При вчиненні випадкових та/або помилкових дій, що можуть призвести до втрати, зміни, поширення, розголошення персональних даних тощо, необхідно:
 - припинити обробку персональних даних;
 - про всі події та факти повідомити безпосереднього керівника та відповідальну особу.
4. При відмові та/або збої програмного забезпечення, за допомогою якого здійснюється обробка персональних даних, працівник зобов’язаний:
 - припинити обробку персональних даних;
 - повідомити безпосереднього керівника та відповідальну особу.
5. При виявленні пошкодження, втрати, викрадення документа або іншого носія персональних даних невідкладно повідомити безпосереднього керівника та відповідальну особу.
6. В разі виникнення надзвичайних ситуацій (пожежа, повінь, стихійні лиха тощо):
 - вжити невідкладних заходів щодо оповіщення відповідних служб реагування;
 - забезпечити збереження носіїв персональних даних осіб від втрати та пошкодження (за наявної можливості та у спосіб, що не загрожує життю та здоров’ю працівників);
 - повідомити безпосереднього керівника та відповідальну особу.
7. Про всі випадки несанкціонованого доступу до персональних даних, передбачені пунктами 1-6 даного Плану, та/або інші випадки, що призвели до пошкодження, псування, несанкціонованого доступу, знищення, поширення тощо персональних даних, працівник, який виявив даний факт, та керівник кредитної спілки невідкладно письмово повідомляють про подію відповідальну особу.

Повідомлення реєструється відповідно до вимог діловодства.
8. Після отримання повідомлення відповідальна особа складає Акт про факт порушення процесу обробки та захисту персональних даних (далі – Акт).

Акт підписується відповідальною особою та працівником, яким виявлено (вчинено) дане порушення. Відмова від підпису працівника фіксується відповідно до вимог чинного законодавства.

Організація роботи, пов'язаної із захистом персональних даних при їхній обробці, тих володільців/розпорядників, на яких не поширюються вимоги частини другої статті 24 Закону України «Про захист персональних даних», покладається безпосередньо на тих осіб, які здійснюють обробку персональних даних.

Вимоги відповідальної особи до заходів щодо забезпечення безпеки обробки персональних даних є обов'язковими для всіх працівників, які здійснюють обробку персональних даних.

Голова правління

О.Г. Бочаров