Процедура
Інтегрованої Системи Управління

ЗАТВЕРДЖЕНО:
Директор
ТОВ «АГРОПРОСПЕРІС»

І.В.Осьмачко

ПР 12-05

Політика інформаційної безпеки

Редакція
2-2019

Зміст

1. ПРИЗНАЧЕННЯ І ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки (далі – Політика) визначає сукупність правил, вимог і керівних принципів в області інформаційної безпеки, якими керується Група компаній «Агропросперіс » (далі – Група) в своїй діяльності, а також визначає основні принципи і завдання системи управління інформаційною безпекою (далі – СУІБ).

1.2. Політика є нормативною основою для захисту інформаційних активів Групи з метою забезпечення:

- конфіденційності – забезпечення доступності до інформації, інформаційних систем та інших програмних процесів тільки для авторизованих користувачів, яким надані для цього відповідні повноваження в мінімально необхідному обсязі;

- цілісності – захисту точності, коректності та повноти інформації та методів її обробки;

- доступності – означає, що авторизований користувач або процес, що має відповідні повноваження, може в будь-який час без особливих проблем отримати доступ до інформаційних систем Групи;

- спостережуваності – забезпечення можливості моніторингу дій користувачів, процесів, які працюють з інформаційними активами Групи, часу і дати такої роботи, а також забезпечення принципу неможливості відмови від виконаних дій.

1.3. Політика заснована на вимогах міжнародних стандартів в області інформаційної безпеки.

1.4. Ця Політика є документом з інформаційної безпеки першого рівня. Документи другого рівня є деталізацією цієї Політики за конкретними напрямами і з конкретних питань (Положення, Правила, Інструкції тощо).

1.5. Ця Політика є обов'язковою для застосування в усіх Компаніях Групи і ознайомлення усіма працівниками і керівництвом Суб'єктів Групи.

2. НОРМАТИВНІ ПОСИЛАННЯ

2.1. Політика розроблена відповідно до міжнародного стандарту ISO / IEK 27001 2013 "Інформаційні технології - Методи захисту - Системи менеджменту інформаційної безпеки - Вимоги".

3. ТЕРМІНИ

3.1. З метою однакового розуміння і належного виконання цієї Політики терміни, визначення, абревіатури, умовні позначення і скорочення мають наступні значення (якщо в тексті Політики прямо не обумовлено інше):

Безпека інформації – захищеність інформації від несанкціонованого та/або небажаного її розголошення (порушення конфіденційності), спотворення (порушення цілісності), втрати або зниження ступеню доступності інформації, а також її незаконного тиражування.

Інформаційні активи – інформація в будь-якому її вигляді, носії інформації, інформаційні системи, телекомунікаційні мережі, програмне забезпечення в будь-якій формі його отримання (придбане або власної розробки), щодо якої необхідно забезпечувати захист відповідно до поставленої мети захисту інформації.

Авторизований користувач – працівник Суб'єкта Групи або третя особа, які мають повноваження використовувати певну інформаційну систему Групи, пройшли реєстрацію і знаходяться в системі під своїм унікальним логіном.

Загроза – реально чи потенційно можливі дії з реалізації небезпечних факторів, що впливають, з метою навмисного або випадкового (ненавмисного) порушення режиму функціонування інформаційних систем і порушення властивостей інформації, що захищається, або інших інформаційних активів.

Уразливість – недолік в інформаційній системі, програмі, обладнанні, використання якого може призводити до порушення цілісності системи та її некоректної роботи. Уразливості з'являються в результаті помилок програмування, недоліків, які допускалися при проектуванні системи, ненадійних паролів, шкідливих програм тощо.

Ризик ІБ – ймовірність того, що певна загроза може бути успішно реалізована, що може завдати шкоди інтересам Групи.

Порушник – особа, яка зробила (намагалася зробити) спробу несанкціонованого доступу до ресурсів системи (спробу виконання заборонених їй дій з даними ресурсом) помилково, через необізнаність або усвідомлено зі злим умислом (з корисливих чи інших мотивів) або без такого (з метою самоствердження тощо) і використовувала для цього різні можливості, методи і засоби.

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління Суб'єкта Групи, заснована на оцінці ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки.

Управління ІБ – циклічний процес, що включає усвідомлення ступеню необхідності захисту інформації та постановку завдань; збір та аналіз даних про стан інформаційної безпеки в рамках Групи; оцінку ризиків ІБ; планування заходів з мінімізації ризиків; реалізацію та впровадження відповідних механізмів контролю, розподіл ролей і відповідальності, навчання персоналу, оперативну роботу по здійсненню захисних заходів; моніторинг функціонування механізмів контролю, оцінку їхньої ефективності та відповідні коригувальні дії.

4. ОБ'ЄКТИ ЗАХИСТУ

4.1. Основними об'єктами захисту системи інформаційної безпеки в Групі є:

- територіально розподілена інформаційна інфраструктура, що включає системи обробки і аналізу інформації, технічні та програмні засоби її обробки, передачі і відображення, в тому числі канали інформаційного обміну і телекомунікації, системи і засоби захисту інформації, об'єкти і приміщення;
- інформаційні системи з обмеженим доступом, а також відкрита (загальнодоступна) інформація, необхідна для роботи Групи, незалежно від форми та виду її надання;
- програмне і апаратне забезпечення бізнес-процесів Групи;
- процеси обробки інформації в інформаційній системі, інформаційні технології, регламенти і процедури збору, обробки, зберігання та передачі інформації, персонал розробників і користувачів системи, а також її обслуговуючий персонал.

5. ОСНОВНІ ПРИНЦИПИ І ЦІЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1. Основною метою системи інформаційної безпеки є захист корпоративних інформаційних систем Групи від можливого збитку в результаті випадкового або навмисного впливу на інформацію, її носії, процеси обробки інформації, зберігання, передачі, а також мінімізація відповідних ризиків.

5.2. Основними завданнями діяльності з забезпечення ІБ Групи є:

- прогнозування і своєчасне виявлення загроз безпеці інформаційних активів Групи, причин і умов, що сприяють завданню шкоди, порушенню бізнес-процесів;
- створення умов функціонування Групи з найменшою вірогідністю реалізації загроз безпеці інформаційних активів і завданню їм шкоди;
- виявлення потенційних загроз у сфері ІБ і вразливостей об'єктів захисту;
- запобігання інцидентів в сфері ІБ;
- створення механізмів і умов оперативного реагування на загрози в сфері ІБ і прояви негативних тенденцій у функціонуванні інформаційних активів Групи;
- створення умов для максимально можливого відшкодування та локалізації збитку, завданого в результаті інцидентів в сфері ІБ;
- підвищення обізнаності працівників Групи, а в окремих випадках – і третіх осіб, в області ризиків, пов'язаних з використанням інформаційних активів Групи, і їх можливих наслідків.

5.3. Побудова системи управління інформаційної безпеки і її функціонування повинні здійснюватися відповідно до таких основних принципів:

- законність (передбачає здійснення захисних заходів та розробку системи безпеки інформації відповідно до чинного законодавства України та міжнародних стандартів безпеки);

- системність (при створенні системи захисту повинні враховуватися всі слабкі і найбільш вразливі місця інформаційної системи, а також характер, можливі об'єкти і напрямки атак на неї з боку порушників, шляхи проникнення в розподілені системи і несанкціонованого доступу до інформації);

- комплексність (комплексне використання методів і засобів захисту комп'ютерних систем передбачає узгоджене застосування різнорідних засобів при побудові цілісної системи захисту, що перекриває всі істотні канали реалізації загроз);

- безперервність захисту (процес забезпечення безпеки інформації, який повинен здійснюватися на постійній основі на всіх рівнях всередині Групи, при цьому кожен працівник Групи повинен брати участь в цьому процесі);

- своєчасність (передбачає упереджувальний характер заходів з забезпечення безпеки інформації);

- вдосконалення (передбачає постійне вдосконалення заходів і засобів захисту інформації);

- розумна достатність (передбачає відповідність рівня витрат на забезпечення безпеки інформації цінності інформаційних ресурсів і величині можливого збитку від їх розголошення, втрати, витоку, знищення та спотворення);

- персональна відповідальність (відповідно до цього принципу розподіл прав і обов'язків працівників будується таким чином, щоб у разі будь-якого порушення коло осіб, причетних до такого порушення, був чітко відомий або зведений до мінімуму);

- мінімізація повноважень (доступ до інформації повинен надаватися тільки в тому випадку і обсязі, якщо це необхідно працівнику для виконання його трудових обов'язків);

- гнучкість системи захисту (система забезпечення інформаційної безпеки повинна бути здатна реагувати на зміни зовнішнього середовища і умов здійснення Групою своєї діяльності);

- простота застосування засобів захисту (механізми і методи захисту повинні бути інтуїтивно зрозумілі і прості у використанні);

- обов'язковість контролю (контроль за діяльністю будь-якого користувача, кожного засобу захисту і щодо будь-якого об'єкта захисту повинен здійснюватися на основі застосування засобів оперативного контролю і реєстрації та повинен охоплювати як несанкціоновані, так і санкціоновані дії користувачів).

5.4. У Групі використовуються наступні вимоги щодо забезпечення інформаційної безпеки:

- періодична інвентаризація авторизованих і неавторизованих пристроїв в корпоративній мережі;

- періодична інвентаризація авторизованого і неавторизованого програмного забезпечення серверів, робочих станцій;

- використання безпечних конфігурацій для апаратного, мережевого і програмного забезпечення, обмеження і контроль мережевих портів;

- управління вразливостями програмного і апаратного забезпечення, їхнє своєчасне усунення (patch management);

- розмежування і періодичний контроль прав доступу користувачів;

- мінімізація і контроль за використанням адміністративних облікових записів;

- ефективний парольний захист;

- захист електронної пошти та веб-браузера;

- захист від шкідливих програм;

- постійний моніторинг та аналіз системних журналів аудиту роботи на всіх рівнях інформаційних систем;

- захист і контроль використання корпоративної мережі;

- можливість відновлення даних;

- криптографічний захист інформації.

6. РОЗПОДІЛ ПОВНОВАЖЕНЬ І ВІДПОВІДАЛЬНОСТІ

6.1. Керівництво Групи здійснює координацію діяльності всіх підрозділів для організації процесів інформаційної безпеки.

6.2. В рамках виконання цієї Політики проводиться регулярний моніторинг і аудит інформаційних систем.

6.3. Керівники Суб'єктів Групи і їхніх структурних підрозділів несуть відповідальність за ознайомлення працівників з вимогами даної Політики.

6.4. Адміністратори інформаційних систем забезпечують безперервне функціонування всіх елементів автоматизованих систем і процесів, а також відповідають за реалізацію заходів, необхідних для реалізації даної Політики.

6.5. Кожен працівник несе відповідальність за дотримання вимог, визначених цією Політикою, іншими чинними в рамках Групи правил, інструкцій, рекомендацій та інших внутрішніх документів щодо забезпечення інформаційної безпеки, а також за своєчасне повідомлення безпосереднього керівництва про всі підозрілі ситуації і можливі інциденти.

6.6. За порушення цієї Політики можуть застосовуватися заходи, передбачені законодавством про працю.

7. ПЕРЕГЛЯД ДОКУМЕНТУ

7.1. Політика переглядається за необхідності при появі та/або зміні інформаційних активів Групи та/або нових технологій, а також у разі зміни законодавчих та інших норм і вимог.