МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

ІНТЕГРОВАНІ СИСТЕМИ УПРАВЛІННЯ ЯКІСТЮ

Навчальний посібник

Харків «ХАІ» 2016

УДК 658.012.32:658.56 (075.8)
ББК 30.607я73
І–73

Колектив авторів:
В. П. Сіроклин, Н. В. Чернобай, Г. Г. Бондаренко, М. В. Глебова, Н. І. Косач

Рецензенти: д-р техн. наук, проф. Г. М. Сучков,
канд. техн. наук, доц. І. В. Григоренко

Інтегровані системи управління якістю [Текст]: навч. посіб. /
І–73 В. П. Сіроклин, Н. В. Чернобай, Г. Г. Бондаренко та ін. – Х.: Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харк. авіац. ін-т», 2016. – 92 с.

ISBN 978-966-662-498-0

Розглянуто поняття інтегрованих систем управління, їхні види, принципи формування і етапи розроблення і впровадження. Наведено перехресні посилання на стандарти, які найчастіше об’єднують в інтегровані системи. Описано вимоги декількох стандартів стосовно систем управління, а саме: ДСТУ OHSAS 18001, ДСТУ ISO 27001, ДСТУ ISO 22000. Подано приклади документованих політик для інтегрованих систем.

Для студентів вищих навчальних закладів, що вивчають курси «Інтегровані системи управління якістю», «Менеджмент якості й елементи системи управління якістю», «Екологічний менеджмент». Може бути корисним для спеціалістів у галузях управління якістю, стандартизації, сертифікації та метрології.

Табл. 3. Бібліогр.: 25 назв

УДК 658.012.32:658.56 (075.8)
ББК 30.607я73

ISBN 978-966-662-498-0

ВСТУП

В останні роки все більш популярним серед вітчизняних організацій постає питання побудови інтегрованих систем управління. Все більше організацій, розробивши і сертифікувавши систему управління якістю, визначають побудову інтегрованої системи управління як наступний крок у вдосконаленні своєї діяльності.

Створення інтегрованої системи управління дозволяє організації одержати ряд переваг, а саме:

- орієнтувати діяльність на сталий стратегічний розвиток з урахуванням вимог і потреб зацікавлених сторін;
- ефективніше використовувати всі види ресурсів, спрямованих на досягнення певних цілей;
- поєднати і взаємозв'язати процеси управління;
- зменшити можливі протиріччя між різними аспектами діяльності;
- знизити витрати на розроблення, функціонування і сертифікацію системи управління якістю організації;
- створити єдину систему навчання і підвищити компетентність персоналу, спрямовану на досягнення певних цілей;
- залучити велику кількість працівників до поліпшення діяльності організації;
- створити єдину систему управління документацією і веденням протоколів;
- підвищити популярність й імідж організації тощо.

Ця система дозволяє організації бути більш впевненою у своїй спроможності поставляти замовникам продукцію, відповідну їх запитам і вимогам.

1 ПОНЯТТЯ, ВИДИ І ЕТАПИ РОЗРОБЛЕННЯ ІНТЕГРОВАНИХ СИСТЕМ УПРАВЛІННЯ

1.1 Поняття і види інтегрованих систем управління

Існує декілька визначень поняття «інтегрована система управління» залежно від сфер діяльності, в яких такі системи створюють або використовують. У сфері управління організацією і забезпечення якості використовують такі визначення:

1) інтегрована система управління (ІСУ) — це сукупність кількох міжнародних стандартів у рамках однієї системи [1];

2) інтегрована система управління — це частина загальної системи управління організації, що відповідає вимогам двох або більше стандартів стосовно системи управління, що функціонує як єдине ціле і спрямована на задоволення зацікавлених сторін.

Основою для створення інтегрованої системи управління на підприємстві є стандарти серії ДСТУ ISO 9000. Це пояснюється тим, що принципи і вимоги стандартів стосовно системи управління якістю схожі з основними принципами і методами загального управління підприємством.

При розробленні й впровадженні ІСУ найчастіше поєднують вимоги ДСТУ ISO 9001 «Система управління якістю. Вимоги» з такими державними і міжнародними стандартами:

- ДСТУ ISO 14001. Система управління навколишнім середовищем;
- ДСТУ OHSAS 18001. Система управління гігієною та безпекою праці;
- ДСТУ ISO 22000. Системи управління безпечністю харчових продуктів. Вимоги до будь-яких організацій харчового ланцюга;
- ДСТУ ISO 27001. Інформаційні технології. Методи та засоби досягнення інформаційної безпеки. Системи управління інформаційною безпекою. Вимоги;
- SA 8000. Соціальна відповідальність;
- ДСТУ ISO/CD 26000. Системи управління соціальною відповідальністю. Вимоги.

Залежно від специфіки діяльності кожного конкретного підприємства інтегровану систему може бути доповнено вимогами стандартів до специфічних систем, наприклад, таких:

- ДСТУ ISO/IEC 17025. Загальні вимоги до компетентності випробувальних і калібрувальних лабораторій;

– ISO 50001. Energy management systems — Requirements with guidance for use (Енергетичний менеджмент. Вимоги та настанова щодо використання);

– ISO 55001. Asset management — Management systems — Requirements (Управління активами. Система управління. Вимоги);

– ДСТУ-П IWA 2. Системи управління якістю. Настанови щодо застосування ISO 9001:2000 у сфері освіти й інші.

Кількість систем, об'єднаних в єдину ІСУ, залежить від потреби, рівня розвитку та ступеня зрілості організації. У таблиці 1.1 наведено приклади максимально можливих комбінацій стандартів залежно від виду економічної діяльності відповідно до класифікації видів економічної діяльності (КВЕД) [14].

Таблиця 1.1

Вид економічної діяльності організації відповідно до класифікатора [14]	**Можлива комбінація стандартів**
Переробна промисловість	ДСТУ ISO 9001+ДСТУ ISO 14001+ +ДСТУ OHSAS 18001+ +ДСТУ ISO/CD 26000+ +SA 8000+специфічний стандарт
Водопостачання; каналізація, поводження з відходами	ДСТУ ISO 9001+ДСТУ ISO 14001+ +ДСТУ OHSAS 18001+ +ДСТУ ISO/CD 26000+SA 8000
Сільське, лісове і рибне господарства	ДСТУ ISO 9001+ДСТУ ISO 14001+ +ДСТУ OHSAS 18001+ДСТУ ISO/CD 26000+SA 8000+ДСТУ ISO 22000
Будівництво	ДСТУ ISO 9001+ДСТУ ISO 14001+ +ДСТУ OHSAS 18001+ +ДСТУ ISO/CD 26000+SA 8000
Оптова й роздрібна торгівля; ремонт автотранспортних засобів і мотоциклів	ДСТУ ISO 9001+ДСТУ ISO 14001+ +ДСТУ OHSAS 18001+ +ДСТУ ISO/CD 26000+SA 8000+ +специфічний стандарт
Фінансова і страхова діяльність	ДСТУ ISO 9001+ДСТУ ISO 14001+ +ДСТУ OHSAS 18001+ +ДСТУ ISO/CD 26000+SA 8000+ +ISO 55001
Тимчасове розміщування і організація харчування	ДСТУ ISO 9001+ДСТУ ISO 14001+ +ДСТУ OHSAS 18001+ДСТУ ISO/CD 26000+SA 8000+ДСТУ ISO 22000

Продовження таблиці 1.1

Вид економічної діяльності організації відповідно до класифікатора [14]	Можлива комбінація стандартів
Інформація й телекомунікації	ДСТУ ISO 9001+ДСТУ ISO 14001+ +ДСТУ OHSAS 18001+ДСТУ ISO/CD 2 6000+SA 8000+ДСТУ ISO 27001+специфічний стандарт
Освіта	ДСТУ ISO 9001+ДСТУ П IWA2+ +ДСТУ ISO27001+ДСТУ ISO 14001+ +ДСТУ OHSAS 18001+ +ДСТУ ISO/CD 26000+SA 8000
Постачання електроенергії, газу, пари і кондиційованого повітря	ДСТУ ISO 9001+ДСТУ ISO 14001+ +ДСТУ OHSAS 18001+ +ДСТУ ISO/CD 26000+SA 8000+ +ISO 50001
Транспорт, складське господарство, поштова й кур'єрська діяльність	ДСТУ ISO 9001+ДСТУ ISO 14001+ДСТУ OHSAS 18001+ +ДСТУ ISO/CD 26000+ +SA 8000+специфічний стандарт
Добувна промисловість і розроблення кар'єрів	ДСТУ ISO 9001+ДСТУ ISO 14001+ +ДСТУ OHSAS 18001+ +ДСТУ ISO/CD 26000+SA 8000+ +специфічний стандарт
Охорона здоров'я і надання соціальної допомоги	ДСТУ ISO 9001+ДСТУ ISO 14001+ +ДСТУ OHSAS 18001+ДСТУ ISO/CD 26000+SA 8000+ +специфічний стандарт

Наведена в таблиці 1.1 послідовність комбінування стандартів дозволить керівникам організацій невдовзі після впровадження ІСУ впорядкувати роботу персоналу в найефективнішому напрямку, а самій організації — вийти на новий рівень якості.

1.2 Особливості й етапи розроблення ІСУ

Практичне створеня інтегрованих систем управління якістю здійснюється за одним з таких варіантів:

1) створення адитивних (від лат. addition – додавання) моделей інтегрованих систем, коли до системи управління якістю, яка виконує роль базової системи, послідовно додають системи управління навколишнім середовищем, системи управління гігієною і безпекою праці, системи управління інформаційною безпекою та ін.;

2) створення повністю інтегрованих моделей, коли декілька систем управління об'єднують в єдиний комплекс одночасно.

Цілісна система управління організацією перш за все має бути спрямована на задоволення максимальної кількості важливих очікувань усіх зацікавлених сторін і мати позитивний економічний ефект. Тому керівництво організації буде прагнути розробити і впровадити відразу декілька систем управління, які будуть інтегровані в єдину систему. Однак такий метод розроблення інтегрованої системи може виявитися занадто складним для організації, що обумовлено труднощами виконання робіт і необхідністю високої кваліфікації персоналу. Тому другий варіант дуже рідко використовують на практиці.

Більш прийнятною в практиці є адитивна модель інтегрування міжнародних систем управління, хоча для її впровадження потрібно більше часу. У зв'язку з цим доцільнішою є послідовна інтеграція в систему окремих складових. Для забезпечення результативності цієї дії наведено перехресні посилання між декількома стандартами (додаток А).

Перш за все у процесі розроблення ІСУ необхідно встановити послідовність кроків інтеграції, адже, починаючи з найбільш важливих складових, в організації визначають основні характеристики системи (структуру процесів, їх форму документування і т.п.), які будуть доповнені й уточнені на наступних етапах. Побудова системи має бути спрямована на найбільш важливі напрямки діяльності організації і сприяти більш серйозному ставленню до цієї системи з боку керівництва і співробітників організації. При виборі складових, які в першу чергу мають бути введені в інтегровану систему управління, в організації слід враховувати такі критерії [2]:

– важливість зацікавленої сторони для організації щодо її місії, системи цінностей, стратегії;

– можливість організації вільно вибирати споживачів, постачальників, співробітників або необхідність боротися за їх лояльність з конкурентами;

– важливість певної групи очікувань для зацікавленої сторони, її вплив на їхню лояльність;

– можливість, інтегрувавши в системі управління одну підсистему, направити її на задоволення очікувань відразу декількох зацікавлених сторін.

Порядок створення інтегрованої системи управління якістю адитивним способом містить такі етапи:

а) аналіз зовнішнього середовища організації, що стосується питань взаємозв'язку зі споживачами, законодавчих та інших вимог до послуг;

б) аналіз діяльності організації, принципів її управління, затвердженної структури;

в) формулювання вимог до інтегрованої системи управління якістю;

г) створення організаційно-нормативної бази інтегрованої системи управління.

Послідовність розширення сфери застосування інтегрованої системи управління може бути такою [2]:

– розроблення та сертифікація системи управління якістю відповідно до вимог ДСТУ ISO 9001;

– інтеграція питань, що стосуються мотивації персоналу (виплати зарплати, соціальної захищеності, можливостей для розвитку та залучення, формування психологічної атмосфери тощо) відповідно до вимог SA 8000;

– інтеграція питань щодо охорони праці та впливу на навколишнє середовище відповідно до вимог ДСТУ OHSAS 18001 і ДСТУ ISO 14001;

– інтеграція питань щодо партнерських відносин зі споживачами і постачальниками;

– інтеграція питань, що стосуються впливів на суспільство, з урахуванням положень ДСТУ ISO/CD 26000.

– інтеграція питань, специфічних для діяльності підприємства.

Ця послідовність може бути іншою залежно від потреб і стратегії організації.

Частину документації ІСУ може бути розроблено як єдиний документ для декількох підсистем. До таких документів належать настанова, політика, методика контролю документації, методика контролю протоколів (записів), методика внутрішнього аудиту і методика коригувальних і попереджувальних дій. Приклади політик інтегрованих систем наведено у додатку Б.

Контрольні запитання

1. Що таке інтегровані системи управління?
2. Яка система є основою для інтегрованих систем управління?
3. Які стандарти найчастіше поєднують в інтегровану систему управління?
4. Який існує принцип формування інтегрованих систем управління?
5. Якими є основні етапи розроблення інтегрованих систем управління?

2 СИСТЕМА УПРАВЛІННЯ ГІГІЄНОЮ І БЕЗПЕКОЮ ПРАЦІ ВІДПОВІДНО ДО ВИМОГ ДСТУ OHSAS 18001

.

2.1 Переваги впровадження системи управління гігієною і безпекою праці

Зі зростанням виробництва і технологічних можливостей збільшується кількість наслідків від аварій, а також небезпека для здоров’я й життя працівників, насамперед тих, що виконують роботи з підвищеною небезпекою. В наш час виробничі компанії прагнуть, з одного боку, зменшити витрати, пов’язані з охороною здоров’я та безпекою праці, з іншого – підвищити безпеку виробництва, ефективно керуючи пов’язаними з ним ризиками для людини.

Створення цілком безпечних і здорових умов праці є одним з найважливіших завдань керівництва підприємства, що нерозривно пов’язано з удосконаленням методів управління охороною праці.

Різні організації є все більш зацікавленими в досягненні і демонстрації вагомої результативності професійної безпеки і здоров'я внаслідок управління професійними ризиками згідно з політикою і цілями в сфері гігієни і безпеки праці (ГіБП). Це пояснюється жорсткістю законодавства, умовами розвитку економічної політики та діями, спрямованими на належне виконання заходів щодо ГіБП, а також постійним загальним зростанням стурбованості зацікавлених сторін питаннями ГіБП.

Багато організацій проводять "аналіз" або "аудит" ГіБП, щоб оцінити їх результативність. Однак самі собою ці "аналізи" і "аудити" є недостатніми для того, щоб забезпечити впевненість у тому, що результативність діяльность організації не тільки відповідає, але й надалі відповідатиме вимогам, які передбачені законом і політикою країни. Щоб були результативними, ці "аналізи" і "аудити" слід проводити в рамках структурованої системи управління, інтегрованої в управління організації.

З цією метою на підприємствах розробляють і впроваджують систему управління гігієною і безпекою праці відповідно до вимог ДСТУ OHSAS 18001 [5].

Система управління ГіБП – це частина загальної системи управління, яка спрямована на ідентифікацію небезпек, оцінювання ризиків та їх управління в сфері професійної безпеки та здоров’я, що пов'язані з діяльністю товариства. Така система управління є інструментом, що дає змогу одержати значні переваги, а саме:

– зменшення кількості випадків заподіяння шкоди персоналу шляхом запобігання небезпечним виробничим факторам на робочих місцях та їх контролю;

– зниження ризику нещасних випадків, що призводять до тяжких наслідків;

– можливість створення інтегрованої системи управління якістю продукції, здоров’ям і безпекою людей, а також екологічного управління;

– забезпечення відповідності діяльності організації законодавству в галузі охорони праці;

– поліпшення іміджу організації.

2.2 Сфера застосування ДСТУ OHSAS 18001

Стандарти OHSAS, що поширюються на управління ГіБП, призначено для забезпечення організацій елементами результативної системи управління ГіБП, які можуть бути інтегровані з іншими вимогами до управління, щоб сприяти організаціям у досягненні цілей щодо ГіБП і економічних цілей. Ці стандарти, так само як й інші міжнародні стандарти, не призначено для використання з метою створення нетарифних бар'єрів у торгівлі або для посилення або зміни зобов'язань, що накладаються на організації законодавством.

У стандарті OHSAS встановлено вимоги до системи управління ГіБП, які дають можливість організації розробити і впровадити політику і цілі, за допомогою яких враховувати законодавчі вимоги і одержувати інформацію про професійні ризики. Цей стардарт можуть застосовувати організації будь-якого типу і розміру з різним географічним положенням, культурними і соціальними особливостями.

ДСТУ OHSAS містить тільки ті вимоги, які можуть бути об'єктивно перевірені під час проведення аудиту. В цьому стандарті не встановлено абсолютні вимоги до результативності системи управління ГіБП, крім зобов’язань стосовно того, що політика в сфері ГіБП має відповідати законодавчим та іншим вимогам, прийнятим в організації для попереджування травм і погіршення здоров'я людей та постійного поліпшення системи управління ГіБП.

У стандарті OHSAS встановлено вимоги до системи управління гігієною і безпекою праці з метою надання допомоги організаціям в управлінні професійними ризиками і підвищенні результативності такого управління. В ньому не зазначено конкретних критеріїв результативності системи управління ГіБП і не подано докладних описів для розроблення системи управління.

Цей стандарт може бути застосовано у будь-якій організації, яка бажає:

а) впроваджувати систему управління гігієною і безпекою праці для усунення або мінімізації ризиків для життя персоналу й інших зацікавлених сторін, які можуть піддаватися ризику, пов'язаному з діяльністю організації;

б) впроваджувати, підтримувати і поліпшувати систему управління ГіБП;

в) переконуватися в тому, що система управління відповідає вимогам визначеної політики в сфері ГіБП,

г) демонструвати відповідність ДСТУ OHSAS шляхом:

- самооцінки і самодекларації;
- підтвердження своєї відповідності сторонами, зацікавленими в організації, такими, як споживачі;
- підтвердження своєї самодекларації зовнішньою відносно організації стороною;
- сертифікації / реєстрації системи управління ГіБП зовнішньою організацією.

Усі вимоги ДСТУ OHSAS призначено для застосування в будь-якій системі управління ГіБП. Їх використання залежить від таких факторів, як політика в сфері ГіБП організації, характер її діяльності і ризиків, а також складності її операцій.

У ДСТУ OHSAS розглянуто питання ГіБП, інші питання щодо сфери здоров'я і безпеки, такі як програми оздоровлення співробітників, безпеки продукції, пошкодження власності або завдання шкоди навколишньому середовищу розгляду не підлягають.

2.3 Терміни і визначення понять стосовно ГіБП

Прийнятний ризик – ризик, зменшений до рівня, який організація може допустити, враховуючи свої законодавчі зобов'язання і власну політику в галузі ГіБП.

Небезпека – джерело, ситуація або дія, які здатні завдати шкоди людині у вигляді травми або погіршення здоров'я, або їх поєднання.

Ідентифікація небезпеки – процес визнання того, що небезпека існує, і визначення її характеристик.

Погіршення здоров'я – розпізнавальний несприятливий фізичний або психічний стан, викликаний і/або посилений робочою діяльністю та/або ситуацією, пов'язаною з роботою.

Інцидент – подія (ї), пов'язана (і) з роботою людини, в результаті якої (их) одержують травму або погіршується здоров'я (безвідносно до ступеня тяжкості) або настає смерть.

Примітка 1. Нещасний випадок – це інцидент, який призвів до підвищення травматизму, погіршення здоров'я або смерті.

Примітка 2. Інцидент, в результаті якого не виникає травм, погіршення здоров'я або настання смерті, може також називатися «промах» або «небезпечна ситуація».

Примітка 3. Аварійна ситуація є особливим видом інциденту.

Гігієна і безпека праці (ГіБП) – умови і чинники, які негативно впливають або можуть впливати на здоров'я і безпеку співробітників, тимчасових працівників, персоналу субпідрядників, відвідувачів і будь-яких інших осіб на робочому місці.

Примітка. На організацію можуть поширюватися законодавчі вимоги, що стосуються здоров'я і безпеки осіб за межами конкретного робочого місця або тих, на кого впливає діяльність на робочому місці.

Система управління ГіБП – частина системи менеджменту організації, яку використовують для розроблення й впровадження її політики у сфері ГіБП, а також для управління ризиками в області ГіБП.

Цілі в сфері ГіБП – цілі, виражені через результативність системи ГіБП, які організація сама встановлює.

Результативність системи управління ГіБП – це вимірні результати управління ризиками організації в області ГіБП.

Політика в сфері ГіБП – загальні наміри організації та її напрями, пов'язані з результативністю системи ГіБП, офіційно сформульовані вищим керівництвом.

Ризик – комбінація ймовірності виникнення небезпечної події або ситуації, що може призвести до травм або погіршення здоров'я людини.

Оцінювання ризиків – процес визначення ризиків, що виникають з небезпек, з урахуванням адекватності існуючих заходів управління та прийняття рішення про допустимість ризику або ні.

Робоче місце – будь-яке фізичне місце розташування, в якому діяльність, пов'язана з роботою, знаходиться під управлінням організації.

2.4 Вимоги до системи управління ГіБП

2.4.1 Загальні вимоги

В організації слід встановлювати, документувати, впроваджувати, підтримувати і постійно поліпшувати систему управління ГіБП відповідно до вимог ДСТУ OHSAS 18001, а також визначати механізми виконання цих вимог. Необхідно також визначати і документувати сферу застосування системи управління ГіБП.

2.4.2 Політика в сфері ГіБП

Найвищому керівництву слід визначати і впроваджувати політику організації у сфері ГіБП і гарантувати, що у встановленій сфері застосування системи управління ГІБП політика відповідає таким вимогам:

а) ураховувати характер і масштаб ризиків у сфері ГіБП організації;

б) містити зобов'язання щодо попередження травм і погіршення здоров'я співробітників, а також щодо постійного поліпшення системи управління ГіБП і її результативності;

в) мати зобов'язання щодо відповідності чинному законодавству та іншим вимогам, які організація зобов'язується виконувати і які належать до небезпек у сфері ГіБП;

г) забезпечувати основу для встановлення і перегляду цілей у сфері ГіБП;

д) бути документально оформленою, впровадженою і постійно підтримуватись;

е) доведеною до всіх осіб, які працюють в організації, з метою сповіщення про їхні індивідуальні зобов'язання в галузі ГіБП;

ж) доступною для зацікавлених сторін;

к) періодично аналізуватися для підтвердження того, що політика залишається актуальною і відповідає діяльності організації.

2.4.3 Планування

2.4.3.1 Ідентифікація небезпек, оцінювання ризиків і визначення заходів управління

В організації слід встановлювати, впроваджувати та виконувати процедури для проведення поточної ідентифікації небезпек, оцінювання ризиків і визначення необхідних заходів управління.

За допомогою процедур для ідентифікації небезпек та оцінювання ризиків слід враховувати:

а) стандартні і нестандартні види діяльності;

б) діяльність всіх осіб, які мають доступ до робочого місця (включаючи субпідрядників і відвідувачів);

в) поведінку людей, їх можливості та інші індивідуальні особливості;

г) ідентифіковані небезпеки, джерело яких не пов'язане з робочим місцем, але які здатні шкідливо впливати на здоров'я і безпеку осіб, що знаходяться в організації;

д) небезпеки, що виникли поблизу робочого місця внаслідок робочої діяльності;

е) інфраструктуру, обладнання та матеріали на робочому місці, надані як організацією, так і іншими підприємствами;

ж) зміни або пропоновані зміни в організації, її діяльності або матеріалах;

к) модифікації системи управління ГіБП, включаючи тимчасові зміни, та їх вплив на операції, процеси і діяльність в організації;

л) будь-які відповідні законодавчі зобов'язання, що стосуються оцінювання ризиків і впровадження необхідних заходів управління;

м) організацію діяльності з розроблення робочих ділянок, процесів, установок, машин, обладнання, операційних процедур, адаптованих до людських можливостей.

Методика організації для ідентифікації небезпек і оцінювання ризиків має бути визначеною з урахуванням сфери застосування, специфіки діяльності й тимчасових факторів і спрямованою більш на попереджування, ніж реагування; забезпечувати ідентифікацію, призначення пріоритетів і документування ризиків, а також використання відповідних заходів управління.

Для управління змінами керівництву організації слід визначити небезпеки й ризики ГіБП, які пов'язані зі змінами в організації, системою менеджменту ГіБП або видами її діяльності до введення цих змін в дії.

В організації слід застосувати результати цього оцінювання при визначенні заходів управління її діяльністю.

При встановленні заходів управління або при розгляді змін існуючих заходів слід враховувати таку їх ієрархію зі скорочення ризиків:

- усунення;
- заміна;
- інженерні заходи управління;
- попередження і/або адміністративне управління;
- індивідуальні засоби захисту.

В організації необхідно документувати і оновлювати результати ідентифікації небезпек, оцінювань ризиків і встановлених заходів управління.

Керівництво організації має гарантувати, що ризики у сфері ГіБП і визначені заходи управління розглядають при встановленні, впровадженні та підтримці системи управління ГіБП.

2.4.3.2 Законодавчі й інші вимоги

В організації слід встановлювати, впроваджувати і виконувати процедури ідентифікації і забезпечення доступу до законодавчих та інших вимог у сфері ГіБП, які застосовуються в організації.

Керівництво організації має гарантувати, що всі законодавчі та інші вимоги, які в організації зобов'язалися виконувати, враховані при установленні, впровадженні й підтримці системи управління ГіБП. Такими вимогами можуть бути закони України і нормативні акти щодо забезпечення безпеки праці на виробництві, санітарно-гігієнічні норми і правила тощо.

В організації слід постійно оновлювати цю інформацію.

Керівництво організації має повідомляти відповідну інформацію щодо законодавчих та інших вимог особам, які працюють під його керівництвом, та іншим відповідним зацікавленим сторонам.

2.4.3.3 Цілі й програма(и) у сфері ГіБП

В організації необхідно встановлювати, впроваджувати і підтримувати документовані цілі в сфері ГіБП у відповідних її пізрозділах і рівнях.

Цілі мають бути вимірними, де це можливо, також узгодженими з політикою в сфері ГіБП, включаючи зобов'язання щодо попередження травм і погіршення здоров'я, дотримання застосовних законодавчих та інших вимог, які організація зобов'язалася виконувати, а також щодо постійного поліпшення системи ГіБП.

При визначенні та аналізі цілей організації слід приймати до уваги законодавчі та інші вимоги, які в організації зобов'язалися виконувати, мати на увазі ризики в сфері ГіБП, розглядати технологічні альтернативи, фінансові, операційні та комерційні вимоги, а також думки відповідних зацікавлених сторін.

В організації слід встановлювати, впроваджувати і підтримувати програму(и) для досягнення визначених цілей. Програма(и) як мінімум має(ють) включати:

- визначення відповідальності і повноважень співробітників для досягнення необхідних цілей щодо відповідних функцій і рівнів організації;
- заходи і графік досягнення цілей.

Програму(и) слід регулярно аналізувати через заплановані інтервали часу і, якщо необхідно, редагувати для гарантованого досягнення цілей.

2.4.4 Впровадження і функціонування

2.4.4.1 Ресурси, ролі, обов'язки, відповідальність і повноваження

Найвище керівництво має взяти на себе повну відповідальність у сфері ГіБП і за систему управління ГіБП і демонструвати свою відповідальність таким шляхом:

а) забезпечення наявності ресурсів (людських, організаційної інфраструктури, технології і фінансів), достатніх для встановлення, впровадження, функціонування та поліпшення системи управління ГіБП;

б) визначення ролей, розподілу відповідальності й підзвітності, делегування повноважень для забезпечення результативності системи управління ГіБП. Ролі, обов'язки, відповідальність і повноваження мають бути задокументовані і доведені до відома співробітників.

Керівництво організації має призначати члена(ів) вищого керівництва з особливою відповідальністю щодо управління ГіБП незалежно від інших обов'язків з установленими ролями і повноваженнями для забезпеченя:

а) встановлення, впровадження і функціонування системи управління ГіБП відповідно до вимог ДСТУ OHSAS 18001;

б) подання вищому керівництву звітів про результативність системи управління ГіБП для аналізу і як основу для її поліпшення.

Призначений(і) вищим керівництвом представник(и) має(ють) бути відомим(ими) всім співробітникам організації.

Усім співробітникам, які мають управлінські обов'язки, слід демонструвати результати функціонування і постійного поліпшення результативності системи управління ГіБП у підпорядкованих їм підрозділах.

Співробітники на робочих місцях є відповідальними за аспекти системи управління ГіБП, якими вони можуть управляти, включаючи дотримання застосовних вимог до системи управління ГіБП в організації.

2.4.4.2 Компетентність, навчання і обізнаність

Керівництву організації слід гарантувати, що всі особи, які виконують під його управлінням завдання і можуть впливати на функціонування системи управління ГіБП, є компетентними, мають відповідну освіту, досвід або підтвердження професійної здатності належними записами.

Слід постійно визначати потреби у навчанні персоналу з питань, які пов'язані з ризиками і системою управління ГіБП. Керівництво організації має забезпечувати проведення цих навчань або застосовувати інші дії, щоб задовольняти ці потреби, оцінювати результативність вжитих засобів і зберігати відповідні записи про це.

В організації необхідно встановлювати, впроваджувати і виконувати процедури, що нададуть можливість співробітникам зрозуміти:

а) які реальні або потенційні наслідки їхньої роботи для системи управління ГіБП можуть виникати залежно від їхнього ставлення до своєї діяльності, відносин у колективі, а також від поліпшення їхньої індивідуальної результативності;

б) свою роль і відповідальність, а також важливість досягнення відповідності політиці в сфері ГіБП, виконання процедур, вимог щодо системи управління ГіБП, включаючи вимоги до готовності й реагування в аварійних ситуаціях;

в) потенційні наслідки відхилень від встановлених процедур.

У процедурах щодо навчання слід враховувати різні рівні:

а) відповідальності, здібностей, мовних навичок і освіченості;

б) ризику.

2.4.4.3 Зв'язок, участь і консультування

2.4.4.3.1 Зв'язок

Щодо небезпек у сфері ГіБП і власної системи управління ГіБП в організації необхідно встановлювати, впроваджувати й виконувати процедури, що стосуються:

а) внутрішнього зв'язку між різними рівнями і функціями організації;

б) зв'язку з підрядниками та іншими відвідувачами робочих місць;

в) отримання, документування відповідних повідомлень від зовнішніх зацікавлених сторін і реагування на них.

2.4.4.3.2 Участь і консультування

В організації слід встановлювати, впроваджувати і виконувати процедури, що забезпечують:

а) участь співробітників шляхом:

- відповідного залучення їх до ідентифікації небезпек, оцінювання ризиків і визначення заходів управління;
- відповідного залучення до розслідування інцидентів;
- залучення до розроблень та аналізу політики і цілей у сфері ГіБП;
- консультування з приводу будь-яких змін, що впливають на систему управління ГіБП;
- представництва при розгляді питань щодо системи управління ГіБП.

Працівників необхідно проінформувати про їхню участь у цих процесах, у тому числі й про те, хто є їх представником (ами) при розгляді питань щодо системи управління ГіБП;

б) консультації з підрядниками з приводу змін, що впливають на функціонування системи управління ГіБП.

Керівництво організації має гарантувати, що за необхідності буде проведено консультації з відповідними зовнішніми зацікавленими сторонами, які мають відношення до системи управління ГіБП.

2.4.4.4 Документація

Документація системи управління ГіБП має містити:

а) політику і цілі у сфері ГіБП;

б) опис сфери застосування системи управління ГіБП;

в) опис основних елементів системи управління ГіБП і їх взаємозв'язків, а також посилання на необхідні документи;

г) документи, зокрема протоколи, які зазначено у ДСТУ OHSAS 18001;

д) документи, зокрема протоколи, які в організації вважають необхідними для забезпечення результативного планування, виконання і управління процесами, що пов'язані з ризиками у сфері ГіБП.

2.4.4.5 Управління документами

Необхідно забезпечити управління документами щодо системи управління ГіБП на основі ДСТУ OHSAS 18001. Управління записами, які являють собою особливий тип документів, слід виконувати відповідно до вимог, наведених у пп. 2.4.5.4.

В організації слід встановлювати, впроваджувати і виконувати такі процедури:

а) затвердження документів, що підтверджує їхню адекватність перед випуском;

б) аналізування і оновлення документів за необхідності, а також повторного їх затвердження;

в) ідентифікації змін і поточного статусу перегляду документів;

г) забезпечення діючих видань відповідних документів на місцях їх використання;

д) забезпечення збереження чіткості документів і простоти ідентифікації;

е) ідентифікації документів зовнішнього походження, визначених організацією як необхідні для планування та функціонування системи управління ГіБП і управління їх розповсюдженням;

ж) запобігання ненавмисному використанню застарілих документів і застосування відповідної ідентифікації документів, якщо вони зберігаються для будь-яких цілей.

2.4.4.6 Управління операціями

В організації слід ідентифікувати ті операції і види діяльності, які пов'язані з ідентифікованими небезпеками, і впроваджувати заходи для управління ризиками у сфері ГіБП, що містять управління змінами.

Для виконання цих операцій і здійснення зазначених видів діяльності в організації необхідно впроваджувати і підтримувати:

а) операційне управління, яке слід інтегрувати в загальну систему управління ГіБП;

б) заходи управління, що пов'язані з продуктами, обладнанням і послугами;

в) заходи управління, що обумовлюють зв'язки з підрядниками та іншими відвідувачами робочих місць;

г) задокументовані методики, в яких відображено ситуації, де їх відсутність може призвести до відхилень від політики і цілей у сфері ГіБП;

д) операційні критерії, відсутність яких може призвести до відхилень від політики і цілей у сфері ГіБП.

2.4.4.7 Готовність до аварійних ситуацій і реагування на них

В організації слід встановлювати, впроваджувати і виконувати такі процедури:

а) ідентифікацію можливих аварійних ситуацій;

б) реагування на ці аварійні ситуації.

Необхідно реагувати на реальні аварійні ситуації і попереджати або пом'якшувати пов'язані з ними несприятливі наслідки у роботі системи управління ГіБП.

При плануванні реагування на аварійні ситуації необхідно враховувати потреби відповідних зацікавлених сторін, наприклад, аварійних служб і сусідів.

В організації також слід періодично проводити перевірку та аналізування актуальності процедури реагування на аварійні ситуації, якщо це практично можливо, включаючи за необхідності відповідні зацікавлені сторони. На основі отриманих результатів і після того, як сталися аварійні ситуації, необхідно коригувати аварійну готовність і процедури реагування, які діють в організації.

2.4.5 Перевірки

2.4.5.1 Вимірювання результативності й моніторинг

В організації необхідно визначати, впроваджувати і підтримувати процедуру(и) для проведення постійного моніторингу та вимірювання результативності в сфері ГіБП. За допомогою таких процедур можна передбачати:

а) якісні й кількісні вимірювання, які відповідають потребам організації;

б) моніторинг ступеня досягнення цілей у сфері ГіБП;

в) моніторинг результативності заходів управління (щодо здоров'я і безпеки);

г) попереджувальні вимірювання результативності для проведення моніторингу відповідності програмі(ам) у сфері ГіБП, заходам управління і операційним критеріям;

д) реагуючі вимірювання результативності для проведення моніторингу погіршення здоров'я, інцидентів (включаючи нещасні випадки, «небезпечні ситуації») та інших доказів недостатньої результативності системи управління ГіБП;

е) запис даних і результатів моніторингу і вимірювань, достатніх для сприяння подальшому аналізуванню коригувальних і запобіжних дій.

Якщо є потрібним обладнання для моніторингу або вимірювання результативності, в організації слід визначати і виконувати процедури калібрування і обслуговування такого обладнання. Необхідно вести записи щодо калібрування, обслуговування і результатів їхнього виконання.

2.4.5.2 Оцінювання відповідності законодавству

2.4.5.2.1 Згідно із зобов'язанням дотримуватися відповідності законодавству слід установлювати, впроваджувати і виконувати процедуру(и) періодичного оцінювання відповідності законодавчим вимогам, які засто-

совуються в організації. Необхідно вести записи результатів періодичного оцінювання.

2.4.5.2.2 В організації слід оцінювати відповідність іншим вимогам, які було прийнято. Можна об'єднати цю оцінку з оцінкою відповідності законодавству або встановити окрему процедуру. Необхідно вести записи результатів періодичного оцінювання.

2.4.5.3 Розслідування інцидентів, невідповідності, коригувальні й запобіжні дії

2.4.5.3.1 Розслідування інцидентів

Керівництво організації має встановлювати, впроваджувати і виконувати процедуру(и) для запису, розслідування і аналізу інцидентів для того, щоб здійснювати такі дії:

а) визначати основні недоліки системи управління ГіБП і чинники, які можуть бути причиною інцидентів або сприяти їхньому виникненню;

б) ідентифікувати потреби в коригувальних діях;

в) визначати можливості запобіжних дій;

г) встановлювати можливості для постійного поліпшення діяльності у сфері ГіБП;

д) інформувати про результати розслідувань.

Розслідування слід проводити своєчасно.

Всі ідентифіковані потреби в коригувальних діях або можливості запобіжних дій необхідно розглядати згідно з пп. 2.4.5.3.2.

Результати розслідування інцидентів мають бути задокументовано і збережено.

2.4.5.3.2 Невідповідності, коригувальні й запобіжні дії

Керівництву організації необхідно встановлювати, впроваджувати і виконувати процедуру розгляду реальних і потенційних невідповідностей, а також процедури прийняття коригувальних і запобіжних дій. В процедурі мають міститись вимоги:

а) до ідентифікації та корекції невідповідностей і прийняття дій для полегшення їх наслідків щодо системи управління ГіБП;

б) розслідування невідповідностей, визначення причин їх появи та проведення дій для виключення їх повторення;

в) оцінювання потреби в діях щодо попередження невідповідностей і впровадження відповідних дій, розроблених для виключення їх виникнення;

г) оформлення записів та інформування про результати вжитих коригувальних і запобіжних дій;

д) аналізу результативності виконаних коригувальних і запобіжних дій.

Якщо коригувальні і запобіжні дії ідентифікують нові або змінені небезпеки або потреби в нових або змінених заходах управління, процедура має містити вимоги щодо оцінювання ризиків запропонованих дій до їхнього впровадження.

Усі коригувальні або запобіжні дії, вжиті для усунення причин реальних або потенційних невідповідностей, мають відповідати масштабу проблеми і бути пропорційними можливим наслідкам ризиків системи управління ГіБП.

Керівництву організації слід гарантувати, що всі необхідні зміни, які є результатом коригувальних або запобіжних дій, внесено в документацію системи управління ГіБП.

2.4.5.4 Управління записами

В організації слід встановлювати і вести записи, які необхідні для демонстрації відповідності вимогам системи управління ГіБП і ДСТУ OHSAS 18001, а також досягнутих результатів. Необхідно також встановлювати, впроваджувати і виконувати процедуру ідентифікації, зберігання, захисту, пошуку, утримування та вилучення записів.

Записи мають бути розбірливими, ідентифікованими і простежуваними.

2.4.5.5 Внутрішній аудит

В організації має бути забезпечено проведення внутрішніх аудитів системи управління ГіБП із запланованою періодичністю для того, щоб здійснити таке:

а) визначити, чи дійсно система управління ГіБП:

1) відповідає запланованим заходам управління ГіБП, включаючи вимоги ДСТУ OHSAS 18001;

2) впроваджена і функціонує як належить;

3) результативна в досягненні політики і цілей організації;

б) надати керівництву організації інформацію про результати аудитів.

Програма аудитів має плануватися, встановлюватися, впроваджуватися і виконуватися співробітниками організації з урахуванням результатів оцінювання ризиків діяльності організації та результатів попередніх аудитів.

Необхідно встановити, впровадити і виконувати процедуру аудиту, яка відображає:

а) відповідальності, компетенції і вимоги щодо планування та проведення аудитів, звітності про результати і ведення відповідних записів;

б) визначення критеріїв, області, періодичності й методів аудиту.

Вибір аудиторів і проведення аудитів мають гарантувати об'єктивність і неупередженість процесу аудиту.

2.4.6 Аналіз з боку керівництва

Найвищому керівництву необхідно переглядати систему управління ГіБП організації із запланованою періодичністю, щоб забезпечити її постійну придатність, адекватність і результативність. Аналіз має містити оцінювання змін для поліпшення системи управління ГіБП, включаючи політику і цілі у сфері ГіБП. Слід вести записи результатів аналізу з боку керівництва.

Вхідні дані аналізу з боку керівництва мають містити:

а) результати внутрішніх аудитів й оцінювання відповідності застосовуваним законодавчим вимогам, а також іншим вимогам, прийнятим організацією;

б) результати участі і консультування;

в) відповідну інформацію від зовнішніх зацікавлених сторін, включаючи скарги;

г) результативність організації в сфері ГіБП;

д) ступінь досягнення цілей;

е) статус розслідування інцидентів, коригувальні й запобіжні дії;

ж) виконання рішень попередніх аналізів з боку керівництва;

к) зміни обставин, включаючи зміни законодавчих та інших вимог, пов'язаних з системою управління ГіБП;

л) рекомендації щодо поліпшення в сфері ГіБП.

Вихідні дані аналізу з боку керівництва мають узгоджуватися із зобов'язаннями організації щодо постійного поліпшення їх і містити всі рішення і дії, пов'язані з можливими змінами:

а) результативності в сфері ГіБП;

б) політики і цілей в сфері ГіБП;

в) ресурсів;

г) інших елементів системи управління ГіБП.

Відповідні результати аналізу з боку керівництва мають бути доступними для поширення та консультування.

Контрольні запитання

1. Яку сферу діяльності організації охоплюють вимоги ДСТУ OHSAS 18001?
2. Що містить система управління ГіБП?
3. Які ресурси є необхідними для функціонування системи управління ГіБП?
4. Які документи є необхідними для функціонування системи управління ГіБП?
5. Якою є процедура внутрішнього аудиту системи управління ГіБП?

6. Якою є послідовність розслідування інцидентів в системі управління ГіБП?

3 СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ВІДПОВІДНО ДО ВИМОГ ДСТУ ISO/IEC 27001

3.1 Переваги впровадження системи управління інформаційною безпекою

Система управління інформаційною безпекою (СУІБ) є сучасним процесом забезпечення безпеки інформаційних ресурсів організації, яка розроблена на основі результатів кращих світових практик. Необхідність впровадження в організаціях стандартів з управління інформаційною безпекою обумовлено вимогами зацікавлених сторін. Впровадження в організаціях цієї системи дозволить:

– оптимізувати вартість побудови та підтримання роботоспроможності системи інформаційної безпеки;

– постійно відслідковувати і оцінювати ризики з урахуванням цілей бізнесу;

– ефективно виявляти найбільш критичні ризики та зменшувати ймовірність їх реалізації;

– розробляти ефективну політику інформаційної безпеки та забезпечувати її якісне виконання;

– ефективно розробляти, впроваджувати і тестувати плани відновлення бізнесу;

– забезпечувати розуміння питань інформаційної безпеки керівництвом і всіма співробітниками організації;

– забезпечувати підвищення репутації та ринкової привабливості організацій;

– зменшувати ризики рейдерських та інших шкідливих для організації атак.

Слід зазначити, що наведені вище переваги не будуть досягнуті лише "формальним" підходом до розроблення, впровадження, функціонування системи управління інформаційною безпекою та незацікавленістю керівництва і співробітників організацій в підвищенні рівня інформаційної безпеки.

3.2 Сфера застосування ДСТУ ISO/IEC 27001

ДСТУ ISO/IEC 27001 [6] розроблено для застосування в організаціях різних типів і визначає вимоги для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримання в робочому стані і поліпшення

документованої СУІБ в контексті загальних ділових ризиків організації. В цьому стандарті встановлено вимоги для реалізації засобів управління захистом, пристосованих до потреб окремих організацій або їх підрозділів.

СУІБ розробляють для того, щоб забезпечити вибір адекватних і пропорційних засобів, які захищають інформаційні активи і надають впевненість зацікавленим сторонам.

Вимоги ДСТУ ISO/IEC 27001 мають загальний характер і призначені для застосування у всіх організаціях незалежно від їх типу, розміру і спрямованості. Виняток будь-якої вимоги є неприйнятним, якщо організація заявляє про відповідність цьому стандарту.

3.3 Терміни і визначення, що стосуються СУІБ

Актив – те, що має цінність для організації.

Доступність – властивість бути прийнятним і придатним до застосування на вимогу вповноваженої особи.

Конфіденційність – підтвердження того, що інформація не є доступною або не є розголошеною неуповноваженим особам, організаціям або процесам.

Захист інформації – збереження конфіденційності, цілісності й доступності інформації; крім того також можуть бути використані інші властивості, такі як автентичність, підзвітність і надійність.

Подія в системі захисту інформації – виявлений випадок, що стосується системи, послуги або стану мережі, який вказує на можливе порушення політики захисту інформації або порушення в роботі засобів захисту, або невідома ситуація, яка може вливати на захист інформації.

Інцидент в системі захисту інформації – одна або серія небажаних або несподіваних подій в системі захисту інформації, які мають великий шанс скомпрометувати ділові операції і поставити під загрозу захист інформації.

Система управління інформаційною безпекою – частина загальної системи менеджменту, основаної на підході ділових ризиків, з метою створювати, впроваджувати, експлуатувати, постійно контролювати, аналізувати, підтримувати в робочому стані і поліпшувати захист інформації.

Цілісність – властивість зберігати точність і повноту активів.

Залишковий ризик – ризик, що залишається після усунення загрози.

Прийняття ризику – рішення взяти на себе ризик.

Аналізування ризику – систематичне використання інформації для виявлення джерел і оцінювання ступеня ризику.

Оцінювання ризику – цілісний процес аналізу ризику і оцінювання його значущості.

Оцінювання значущості ризику – процес порівняння розрахункового ризику із заданими критеріями ризику з метою визначити рівень впливу ризику на діяльність організації.

Управління ризиками – узгоджені види діяльності з керівництва і управління організацією щодо ризиків.

Оброблення ризику – процес вибору і реалізації заходів щодо зміни ризику.

Заява про застосовність – документована заява, що описує цілі й засоби управління відносно СУІБ організації.

Примітка. Цілі й засоби управління грунтуються на результатах і висновках оцінювання ризиків і процесу оброблення ризиків, законодавчих або нормативних вимогах, договірних зобов'язаннях і ділових вимогах захисту інформації організації.

3.4 Середовище організації

3.4.1 Розуміння потреб і очікувань зацікавлених сторін

Керівництву організації слід визначити таке:

а) зацікавлені сторони, які впливають на систему управління інформаційною безпекою;

б) вимоги цих зацікавлених сторін, які є доречними й стосуються системи управління інформаційною безпекою.

В організації необхідно проводити моніторинг і аналізування інформації про ці зацікавлені сторони і їхні відповідні вимоги.

Примітки. Вимоги зацікавлених сторін можуть містити законодавчі, нормативні вимоги і договірні зобов'язання.

3.4.2 Визначення сфери застосування системи управління інформаційною безпекою

Керівництво організації має визначити межі й застосовність системи управління інформаційною безпекою, щоб установити її сферу застосування.

Визначаючи цю сферу застосування, керівництво організації має розглянути таке:

а) зовнішні й внутрішні чинники;

б) вимоги відповідних зацікавлених сторін;

в) інтерфейси і залежності між діяльністю цієї організації й діяльністю інших організацій .

Сфера застосування має бути оформлена документально й бути доступною.

3.4.3 Система управління інформаційною безпекою

В організації слід розробляти, запроваджувати, підтримувати й постійно поліпшувати систему управління інформаційною безпекою відповідно до вимог ДСТУ ISO 27001.

3.5 Лідерство

3.5.1 Лідерство і зобов'язання

Найвищому керівництву організації слід демонструвати своє лідерство та своє зобов'язання щодо системи управління інформаційною безпекою таким шляхом:

а) забезпечуючи розроблення політики і цілей у сфері інформаційної безпеки і їх узгодженість зі стратегічним напрямком і середовищем організації;

б) забезпечуючи інтегрування вимог системи управління інформаційною безпекою в бізнес-процеси організації;

в) забезпечуючи наявність ресурсів, потрібних для результативного функціювання системи управління інформаційною безпекою;

г) інформуючи персонал про важливість результативного управління інформаційною безпекою та відповідності вимогам системи управління інформаційною безпекою;

д) забезпечуючи досягнення системою управління інформаційною безпекою запланованих результатів;

е) залучаючи, спрямовуючи та заохочуючи персонал до постійного підвищення результативності системи управління інформаційною безпекою;

ж) сприяючи поліпшуванню СУІБ;

з) підтримуючи інших відповідних керівників для демонстрування їхнього лідерства в їх сферах відповідальності.

3.5.2 Політика

Найвищому керівництву організації необхідно сформувати, запровадити і актуалізувати політику у сфері інформаційної безпеки. Ця політика має містити:

а) відповідність призначеності й середовищу організації і її стратегічному напрямку;

б) основу для встановлення цілей у сфері якості;

в) зобов'язання стосовно задоволення вимог щодо інформаційної безпеки;

г) зобов'язання щодо постійного поліпшування системи управління інформаційною безпекою.

Політика у сфері інформаційної безпеки має бути такою:

а) доступною і актуалізованою у формі задокументованої інформації;

б) доведеною до відома співробітників, зрозумілою та застосованою в межах організації;

в) доступною для відповідних зацікавлених сторін.

3.5.3 Функції, обов'язки і повноваження в межах організації

Найвищому керівництву організації необхідно забезпечити, щоб обов'язки і повноваження відповідних посадових осіб, які мають відношення до інформаційної безпеки, було встановлено, доведено до їх відома та зрозуміло визначено в межах організації.

Слід встановити виконання таких дій:

а) забезпечення відповідності системи управління інформаційною безпекою вимогам ДСТУ ISO 27001;

б) звітування про дієвість системи управління інформаційною безпекою та можливості для її поліпшення, зокрема перед найвищим керівництвом.

Примітка. Найвище керівництво організації може розподіляти і делегувати повноваження щодо постійного інформування стосовно результативності системи управління інформаційною безпекою декільком відповідальним особам.

3.6 Планування

3.6.1 Дії стосовно ризиків і можливостей

3.6.1.1 Під час планування системи управління інформаційною безпекою керівництво організації має розглянути зовнішні й внутрішні чинники, вимоги споживачів і зацікавлених сторін, а також визначити ризики і можливості, які потрібно врахувати, щоб виконати такі дії:

а) забезпечити впевненість у тому, що система управління інформаційною безпекою може досягти запланованого(-их) результату(-ів);

б) збільшити кількість бажаних ефектів;

в) запобігти небажаним ефектам або зменшити їхню кількість;

г) досягти її поліпшення.

Керівництво організації має планувати таке:

а) дії стосовно цих ризиків і можливостей;

б) спосіб, яким можна:

1) інтегрувати і запроваджувати дії щодо процесів системи управління інформаційною безпекою;

2) оцінювати результативність цих дій.

3.6.1.2 Оцінювання ризиків інформаційної безпеки

В організації слід визначити і впровадити процес оцінювання ризиків інформаційної безпеки, на основі якого має бути:

а) встановлено й підтримано критерії виявлення ризиків щодо інформаційної безпеки, які містять:

1) критерії прийняття ризиків;

2) критерії оцінювання ризиків щодо інформаційної безпеки;

б) забезпечено, що повторне оцінювання ризиків щодо інформаційної безпеки дозволить отримати логічні обґрунтовані результати, які можна порівняти між собою;

в) визначено ризики щодо інформаційної безпеки, а саме:

1) застосовано процес оцінювання ризиків щодо інформаційної безпеки для виявлення ризиків, які пов'язані з втратою конфіденційності, цілісності й доступності інформації в межах системи управління інформаційною безпекою;

2) визначено відповідальних за ризики;

г) проаналізовано ризики щодо інформаційної безпеки, а саме:

1) встановлено потенційні наслідки, які можуть виникнути через ризики, які вказано в п. 3.6.1.2, в, 1;

2) визначено реалістичну вірогідність виникнення ризиків, які вказано в п. 3.6.1.2, в, 1;

3) встановлено рівні ризику;

д) оцінено ризики щодо інформаційної безпеки, а саме:

1) порівняно результати аналізування ризиків з визначеними критеріями, які вказано п. 3.6.1.2, а;

2) встановлено пріоритети щодо оброблення ризиків для подальшого їхнього аналізування.

В організації слід зберігати задокументовану інформацію стосовно процесу оцінювання ризиків щодо інформаційної безпеки.

3.6.1.3 Управління ризиками щодо інформаційної безпеки

В організації слід визначити і впровадити процес управління ризиками щодо інформаційної безпеки, на основі якого має бути:

а) вибрано відповідний метод управління ризиками щодо інформаційної безпеки з врахуванням результатів оцінювання ризиків;

б) визначено всі елементи управління, які є необхідними для реалізації вибраного методу управління ризиками щодо інформаційної безпеки.

Примітка. В організації за потребою можуть бути розроблені власні елементи управління або визначені з будь-якого джерела;

в) порівняно всі елементи управління, які вказано в п. 3.6.1.3, б, з тими, які наведено в додатку В, для того, щоб впевнитися, що всі необхідні елементи були враховані;

г) розроблено Положення про застосування (SoA), яке містить необхідні елементи управління і обґрунтування їхнього внесення у перелік, а також виключення будь-яких елементів управління з переліку, який наведено у додатку В.

В організації слід зберігати задокументовану інформацію стосовно процесу управління ризиками щодо інформаційної безпеки.

3.6.2 Цілі у сфері інформаційної безпеки і планування дій для їх досягнення

3.6.2.1 Керівництво організації має встановити цілі у сфері інформаційної безпеки для відповідних підрозділів, рівнів і процесів, необхідних для функціонування системи управління інформаційною безпекою.

Потрібно, щоб цілі у сфері якості були такі:

а) узгоджені з політикою у сфері інформаційної безпеки;

б) вимірні;

в) ураховували застосовні вимоги, результати оцінювання і оброблення ризиків;

г) доведені до відома персоналу;

д) актуалізовані, як належить.

Організація має підтримувати в актуальному стані задокументовану інформацію щодо цілей у сфері інформаційної безпеки.

3.6.2.2 Плануючи те, як досягти своїх цілей у сфері інформаційної безпеки, керівництво організації має визначати таке:

а) що потрібно робити;

б) які ресурси будуть потрібні;

в) хто буде відповідальним;

г) коли це буде завершено;

д) як оцінюватимуть результати.

3.7 Підтримання системи управління інформаційною безпекою

3.7.1 Ресурси

Керівництво організації має визначити ресурси, потрібні для розроблення, запроваджування, підтримування та постійного поліпшування системи управління інформаційною безпекою, та забезпечити їх наявність.

3.7.2 Компетентність

Керівництву організації необхідно виконувати таке:

а) визначати необхідну компетентність персоналу, який самостійно виконує роботу, що впливає на дієвість і результативність системи управління інформаційною безпекою;

б) забезпечувати впевненість у тому, що компетентність цих осіб ґрунтується на належній освіті, професійній підготовленості або досвіді;

в) там, де застосовно, вживати заходів для набуття необхідної компетентності й оцінювати результативність ужитих заходів;

г) зберігати належну задокументовану інформацію як доказ компетентності.

Примітка. Застосовані заходи можуть охоплювати, наприклад, навчання, наставництво, переведення персоналу на нові посади або прийняття компетентних осіб на роботу чи укладання з ними контрактів.

3.7.3 Обізнаність

Керівництво організації має забезпечувати, щоб особи, які виконують роботу під його контролем, були обізнаними щодо такого:

а) політики у сфері інформаційної безпеки;

б) відповідних цілей у сфері інформаційної безпеки;

в) свого внеску у результативність системи управління інформаційною безпекою, зокрема вигід від поліпшення показників діяльності;

г) наслідків невиконання вимог системи управління інформаційною безпекою.

3.7.4 Інформування

Керівництво організації має визначати потреби щодо внутрішнього і зовнішнього інформування, які є доречними для системи управління інформаційною безпекою, зокрема:

а) про що інформувати;

б) коли інформувати;

в) кого інформувати;

г) як інформувати;

д) хто має інформувати.

3.7.5 Задокументована інформація

3.7.5.1 Загальні положення

Необхідно, щоб система управління інформаційною безпекою організації охоплювала таке:

а) задокументовану інформацію, яку потребує ДСТУ ISO 27001;

б) задокументовану інформацію, яку організація вважає необхідною для результативності системи управління інформаційною безпекою.

Примітка. Обсяг задокументованої інформації для системи управління інформаційною безпекою в різних організаціях може бути різним залежно від такого:

– розміру організації, її виду діяльності, її процесів, продукції та послуг;

складності процесів та їхніх взаємодій;

– компетентності персоналу.

3.7.5.2 Створювання і актуалізування

Під час створювання і актуалізування задокументованої інформації співробітники організації мають забезпечувати таке:

а) належні ідентифікацію і опис (наприклад, назву, дату, прізвище автора, номер для посилання);

б) належний формат (наприклад, мову, версію програмного засобу, графічні зображення) і носії (наприклад, паперовий, електронний);

в) належний аналіз і схвалення з погляду придатності й адекватності.

3.7.5.3 Контроль задокументованої інформації

3.7.5.3.1 Задокументовану інформацію, яка необхідна для функціонування системи управління інформаційною безпекою і яку визначено в ДСТУ ISO 27001 слід контролювати для забезпечення такого:

а) її наявності й придатності до використання, зазначення де і коли вона може бути потрібною;

б) її адекватної захищеності (наприклад, від утрати конфіденційності, неналежного використання або втрати цілісності).

3.7.5.3.1 Для контролю задокументованої інформації співробітники організації мають вдаватися до таких дій:

а) розподілу, доступу, пошуку і використання;

б) збереження, зокрема збереження її розбірливості;

в) контролю змін (наприклад, контролю версії);

г) зберігання та вилучання.

Задокументовану інформацію зовнішнього походження, яку в організації вважають необхідною для планування та функціювання системи управління інформаційною безпекою, слід ідентифікувати у належний спосіб і контролювати.

Задокументовану інформацію, яку зберігають як доказ відповідності, потрібно захищати від ненавмисного змінення.

Примітка. Доступ до задокументованої інформації може передбачати рішення про дозвіл лише на ознайомлення з нею або про дозвіл на ознайомлення з нею та повноваження щодо внесення змін до неї.

3.8 Експлуатація

3.8.1 Оперативне планування і контроль

Керівництву організації слід планувати, запроваджувати та контролювати процеси, потрібні для задоволення вимог щодо інформаційної безпеки і реалізації дій, які визначені в п. 3.6.1. В організації мають виконуватися плани стосовно досягнення цілей щодо інформаційної безпеки, які зазначені у п. 3.6.2. Необхідно, щоб результати цього планування зберігалися в обсязі, який є достатнім для отримання впевненості в тому, що процеси будуть виконуватися, як заплановано.

Керівництво організації має контролювати заплановані зміни і аналізувати наслідки непередбачених змін і, за потреби, виконувати дії, щоб послабити будь-які їхні несприятливі впливи.

В організації слід забезпечувати контролювання процесів, які було передано сторонньому виконавцеві.

3.8.2 Аналізування ризиків щодо інформаційної безпеки

Керівництво організації має забезпечити аналізування ризиків щодо інформаційної безпеки через заплановані проміжки часу або у випадку, коли є можливими або вже проходять суттєві зміни з урахуванням критеріїв, які вказано у п. 3.6.1.2, а.

В організації слід зберігати задокументовану інформацію про результати аналізування ризиків щодо інформаційної безпеки.

3.8.3 Контролювання ризиків щодо інформаційної безпеки

Керівництво організації має забезпечити виконання плану управління ризиками щодо інформаційної безпеки.

В організації слід зберігати задокументовану інформацію про результати контролювання виконання запланованих дій з управління ризиками щодо інформаційної безпеки.

3.9 Оцінювання результативності

3.9.1 Моніторинг, вимірювання, аналізування і оцінювання

Керівництво організації має оцінювати стан інформаційної безпеки і результативності системи управління інформаційною безпекою.

В організації має бути визначено таке:

а) що слід піддавати моніторингу й вимірюванню, включаючи процеси інформаційної безпеки і елементи управління;

б) методи моніторингу, вимірювання, аналізування і оцінювання, потрібні для забезпечення вірогідних результатів;

в) коли треба проводити моніторинг і вимірювання;

г) хто має проводити моніторинг і вимірювання;

д) коли треба аналізувати і оцінювати результати моніторингу та вимірювання;

е) хто має аналізувати і оцінювати ці результати.

В організації слід зберігати відповідну задокументовану інформацію як доказ отриманих результатів моніторингу й вимірювань.

3.9.2 Внутрішній аудит

3.9.2.1 В організації необхідно проводити внутрішні аудити в заплановані проміжки часу для отримання інформації про те, чи система управління інформаційною безпекою:

а) відповідає:

1) прийнятим в організації вимогам до цієї системи;

2) вимогам ДСТУ ISO 27001;

б) результативно запроваджена та її підтримують.

3.9.2.2 В організації слід виконувати таке:

а) планувати, розробляти, виконувати і актуалізувати програму аудиту, охоплюючи періодичність, методи, відповідальність, вимоги щодо планування і звітність. Потрібно, щоб у програмі аудиту було враховано важливість процесів, яких це стосується, зміни, що впливають на діяльність організації, і результати попередніх аудитів;

б) визначати критерії аудиту й сферу застосування кожного аудиту;

в) добирати аудиторів і проваджувати аудити так, щоб було забезпечено об’єктивність і неупередженість процесу аудиту;

г) забезпечувати звітування про результати аудитів перед відповідним керівництвом;

д) виконувати відповідні коригування і коригувальні дії без необґрунтованої затримки;

е) зберігати задокументовану інформацію як доказ виконання програми аудиту і отриманих результатів аудиту.

3.9.3 Аналізування системи управління інформаційною безпекою

3.9.3.1 Загальні положення

Найвищому керівництву слід із запланованою періодичністю аналізувати запроваджену в організації систему управління інформаційною безпекою, щоб забезпечувати її постійну придатність, адекватність, результативність і узгодженість із стратегічним напрямом організації.

3.9.3.2 Вхідні дані аналізування системи управління інформаційною безпекою

Аналізування системи управління інформаційною безпекою необхідно планувати і провадити з урахуванням такого:

а) статусу дій за результатами попередніх аналізів системи управління інформаційною безпекою;

б) змін у зовнішніх і внутрішніх чинниках, доречних для цієї системи управління;

в) інформації про дієвість і результативність системи управління інформаційною безпекою, охоплюючи тенденції стосовно такого:

1) результатів досягнення цілей у сфері інформаційної безпеки;

2) невідповідностей і коригувальних дій;

3) результатів моніторингу та вимірювання;

4) результатів аудитів;

г) зворотнього зв'язку із зацікавленими сторонами;

д) результативності дій, виконаних щодо ризиків і можливостей;

е) можливостей для поліпшення.

3.9.3.3 Вихідні дані аналізування системи управління інформаційною безпекою

Необхідно забезпечувати, щоб вихідні дані аналізування системи управління охоплювали рішення та дії стосовно такого:

а) можливостей для поліпшення роботи системи;

б) будь-якої потреби у змінах системи управління інформаційною безпекою.

В організації слід зберігати задокументовану інформацію як доказ результатів аналізування системи управління інформаційною безпекою.

3.10 Поліпшування

3.10.1 Невідповідність і коригувальні дії

3.10.1.1 У разі виникнення невідповідності керівництво організації має:

а) реагувати на невідповідність і, залежно від обставин, а саме:

1) виконувати дії щодо її контролювання та коригування;

2) приймати рішення щодо наслідків;

б) оцінювати потребу в діях щодо усунення причин(-и) невідповідності з тим, щоб вона не виникала повторно або в іншому місці, а саме:

1) аналізуючи невідповідність;

2) визначаючи причини невідповідності;

3) встановлюючи наявність подібних невідповідностей або потенційну можливість їх виникнення;

в) виконувати будь-які потрібні дії;

г) аналізувати результативність будь-якої виконаної коригувальної дії;

д) за потреби, оновлювати перелік ризиків та можливостей, які були визначені під час планування;

е) за потреби, вносити зміни до системи управління інформаційною безпекою.

Необхідно забезпечувати, щоб коригувальні дії відповідали наслідкам виявлених невідповідностей.

3.10.1.2 В організації слід зберігати задокументовану інформацію як доказ щодо:

а) характеру невідповідностей і будь-яких подальших виконаних дій;

б) результатів будь-якої коригувальної дії.

3.10.2 Постійне поліпшування

Керівництво організації має забезпечувати постійне поліпшування придатності, адекватності і результативності системи управління інформаційною безпекою.

Контрольні запитання

1. Які переваги має організація від впровадження СУІБ?
2. Які основні дії слід впроваджувати щодо моніторингу і аналізу роботи СУІБ?
3. Які основні дії мають бути описані в процедурі контроля документів СУІБ?
4. Що треба зробити при розробленні СУІБ?
5. Що мають містити вхідні дані для аналізу СУІБ з боку керівництва?
6. Які вимоги визначає процедура коригувальних дій?

4 СИСТЕМА УПРАВЛІННЯ БЕЗПЕЧНІСТЮ ХАРЧОВИХ ПРОДУКТІВ ВІДПОВІДНО ДО ВИМОГ ДСТУ ISO 22000

4.1 Переваги впровадження системи управління безпечністю харчових продуктів

Безпечність харчових продуктів пов’язана з наявністю небезпечних чинників у харчових продуктах на момент споживання (вживання споживачем). Оскільки небезпечний чинник харчового продукту може з’явитися на

будь-якій ланці харчового ланцюга, адекватне керування в усьому харчовому ланцюзі є суттєво важливим. Отже, харчові продукти можна убезпечити спільними зусиллями всіх сторін, що беруть участь у харчовому ланцюзі.

Харчовий ланцюг охоплює різноманітні організації: від виробників кормів і первинної продукції до виробників харчових продуктів, операторів з їх транспортування та зберігання і субпідрядників і далі до підприємств роздрібної торгівлі й закладів громадського харчування (разом із суміжними організаціями, такими як виробники устаткування, пакувальних матеріалів, мийних засобів, добавок та інгредієнтів). Такий ланцюг охоплює також організації з надання послуг.

Інформування в усьому харчовому ланцюзі є суттєвим для забезпечення ідентифікації та адекватного керування всіма відповідними небезпечними чинниками харчового продукту на кожній ланці в межах харчового ланцюга. Це передбачає обмін інформацією між організаціями, що перебувають як вище, так і нижче в харчовому ланцюзі. Інформування замовників і постачальників про ідентифіковані небезпечні чинники та заходи керування допоможе зробити зрозумілішими вимоги замовників і постачальників (наприклад, стосовно можливості задоволення вимог і потреби в таких вимогах та їх впливу на кінцевий продукт).

Розпізнавання ролі та місця організації в харчовому ланцюзі є необхідним для забезпечення результативного взаємодійового (інтерактивного) інформування в усьому харчовому ланцюзі задля поставляння кінцевому споживачеві безпечних харчових продуктів.

Найбільш результативними є системи управління безпечністю харчових продуктів, які встановлюють, застосовують і поновлюють у межах структурованої системи управління та долучають до загальної діяльності з керування організацією.

4.2 Сфера застосування ДСТУ ISO 22000

У ДСТУ ISO 22000 установлено вимоги до системи управління безпечністю харчових продуктів, якщо організація, яка є частиною харчового ланцюга, має необхідність продемонструвати свою здатність керувати небезпечними чинниками харчових продуктів для гарантування того, що харчовий продукт є безпечним на момент його споживання людиною.

Стандарт можуть застосовувати всі організації незалежно від розміру, які залучені до будь-якої ключової частини харчового ланцюга та бажають запровадити системи, які гарантують постійний випуск безпечних продуктів. Засоби виконання будь-яких вимог цього стандарту можна отримати, використовуючи внутрішні та/або зовнішні ресурси.

У стандарті встановлено вимоги, які дають змогу організації виконувати такі дії:

а) планувати, запроваджувати, використовувати, підтримувати і оновлювати систему управління безпечністю харчових продуктів, спрямовану на постачання продуктів, які в разі використання за призначеністю є безпечними для споживача;

б) демонструвати відповідність застосовним законодавчим і нормативним вимогам до безпечності харчових продуктів;

в) визначати і оцінювати вимоги замовників і демонструвати відповідність таким взаємоузгодженим вимогам, які стосуються безпечності харчових продуктів, для підвищення задоволеності замовників;

г) результативно інформувати про проблеми безпечності харчових продуктів своїх постачальників, замовників і відповідні зацікавлені сторони у межах харчового ланцюга;

д) забезпечувати відповідність дій організації своїй заявленій політиці щодо безпечності харчових продуктів;

е) демонструвати таку відповідність зацікавленим сторонам;

ж) прагнути сертифікації або реєстрації своєї системи управління безпечністю харчових продуктів зовнішньою організацією або провадити самооцінювання або самодекларування відповідності системи цьому стандарту.

Усі вимоги цього стандарту є загальними і придатними для застосовування всіма організаціями харчового ланцюга незалежно від їх розміру та складності. До них належать організації, що безпосередньо або опосередковано залучені до однієї або кількох ланок харчового ланцюга. Організації, які залучені безпосередньо, охоплюють, не обмежуючись наведеним, виробників кормів, збиральників урожаю, фермерів, виробників інгредієнтів, виробників харчових продуктів, роздрібних торгівців, заклади громадського харчування, постачальників продукції, організації, що надають послуги з миття та дезінфікування, транспортування, зберігання і розподіляння продукції. До інших організацій, які залучені опосередковано, належать, не обмежуючись наведеним, постачальники устаткування, мийних і дезінфікувальних засобів, пакувальних та інших матеріалів, що контактують з харчовими продуктами.

Цей стандарт дозволяє малим або менш розвиненим організаціям (наприклад, дрібній фермі, дрібному пакувальнику-дистриб'ютору, невеликому підприємству роздрібної торгівлі або невеликому закладу громадського харчування) впроваджувати зовні розроблену комбінацію заходів керування.

4.3 Терміни і визначення понять, що застосовуються у системі управління безпечністю харчових продуктів

Безпечність харчових продуктів – поняття, що харчовий продукт не завдасть шкоди споживачеві, якщо його виготовлено та / або спожито в їжу відповідно за призначеністю.

Харчовий ланцюг – послідовність стадій і певних операцій виготовлювання, оброблювання, розподіляння, зберігання харчових продуктів та їхніх інгредієнтів і користування ними, починаючи з первинного виробництва і закінчуючи споживанням.

Примітка 1. До цього належить виробництво кормів для тварин, які дають харчові продукти, та для тварин, призначених для виробляння харчових продуктів.

Примітка 2. Харчовий ланцюг також охоплює виробництво матеріалів, які за своєю призначеністю контактуватимуть з харчовими продуктами або сировиною.

Небезпечний чинник харчового продукту – біологічний, хімічний або фізичний компонент у харчовому продукті або стан харчового продукту, що потенційно може спричинити негативний вплив на здоров'я людини.

Політика щодо безпечності харчових продуктів – загальні наміри та спрямованість організації стосовно безпечності харчових продуктів, що офіційно висловлені найвищим керівництвом.

Кінцевий продукт – продукт, який не буде піддано жодному подальшому обробленню або перетворенню.

Примітка. Продукт, який буде піддано подальшому обробленню або перетворенню іншою організацією, є кінцевим продуктом для першої організації та сировиною або інгредієнтом для другої організації.

Блок-схема процесу – схематичне і систематизоване зображення послідовності й взаємодії стадій.

Захід керування (безпечністю харчових продуктів) – дія або комплекс дій, які можна застосовувати для запобігання або усунення небезпечного чинника харчового продукту або для його зменшення до прийнятного рівня.

Програма-передумова (ПП); програма, необхідна як умова (безпечності харчових продуктів) – базові умови та діяльність, необхідні для підтримання потрібного рівня гігієни навколишнього середовища у всьому харчовому ланцюзі, придатному для виробництва, оперування та постачання безпечних кінцевих продуктів і безпечних харчових продуктів для споживання людиною.

Примітка. Потрібні ПП залежать від сегмента харчового ланцюга, в якому працює організація, та типу організації. Приклади відповідних термінів: Належна сільськогосподарська практика (GAP), Належна ветеринарна практика (GVP), Належна виробнича практика (GMP), Належна гігієнічна практика (GHP), Належна практика первинного виробництва (GPP), Належна дистриб'юторська практика (GDP) і Належна торговельна практика (GTP)

Операційна ПП – програма-передумова, яка була ідентифікована під час аналізу небезпечних чинників як суттєво важлива, щоб керувати ймовірністю привнесення небезпечних чинників до харчового продукту та / або забруднення продукту, або розповсюдження небезпечних чинників у продукті або середовищі його оброблення.

Критична точка керування (КТК) (безпечністю харчових продуктів) – стадія, на якій можна здійснювати керування і яка є суттєвою для запобігання або усунення небезпечного чинника харчового продукту або його зниження до прийнятного рівня.

Критична межа – критерій, що відділяє прийнятне від неприйнятного.

Моніторинг – проведення запланованої послідовності спостережень або вимірювань, щоб оцінити, чи функціонують заходи керування як призначено.

Підтвердження, валідація (безпечності харчових продуктів) – отримання доказів того, що заходи керування в рамках плану НАССР та операційних ПП можуть бути результативними.

Перевіряння, верифікація – підтвердження наданням об'єктивних доказів, що встановлені вимоги дотримано.

Оновлення – негайні та / або заплановані дії для забезпечення використання найновішої інформації.

4.4 Система управління безпечністю харчових продуктів. Вимоги

4.4.1 Загальні вимоги

В організації слід установлювати, документувати, проваджувати і підтримувати результативну систему управління безпечністю харчових продуктів та оновлювати її, за потреби, відповідно до вимог цього стандарту.

Керівництву організації необхідно визначати сферу застосування системи управління безпечністю харчових продуктів. У сфері застосування слід вказати продукти і категорії продуктів, процеси і виробничі ділянки, охоплені системою управління безпечністю харчових продуктів.

Співробітники організації мають виконувати такі дії:

а) забезпечувати, щоб небезпечні чинники, які з достатньою ймовірністю можуть виникнути в продуктах, охоплених системою управління безпечністю харчових продуктів, було проідентифіковано, оцінено та проконтрольовано таким чином, щоб продукти, вироблені цією організацією ніяк, ані безпосередньо, ані опосередковано, не зашкодили споживачеві;

б) повідомляти відповідну інформацію з питань безпечності своїх продуктів у межах харчового ланцюга;

в) інформувати про створення, запровадження і оновлення системи управління безпечністю харчових продуктів всіх співробітників організації в обсязі, необхідному для убезпечення харчових продуктів згідно з вимогами ДСТУ ISO 22000;

г) періодично оцінювати і, за потреби, оновлювати систему управління безпечністю харчових продуктів, щоб гарантувати, що система відображає діяльність організації і охоплює найновішу інформацію щодо небезпечних чинників харчового продукту, які підлягають керуванню.

Якщо для будь-якого процесу, який може вплинути на відповідність кінцевого продукту, в організації вибрано стороннього виконавця, керівництво організації має забезпечити управління такими процесами.

Елементи керування такими субпідрядними процесами має бути визначено і задокументовано в межах системи управління безпечністю харчових продуктів.

4.4.2 Вимоги до документації

4.4.2.1 Загальні положення

Документація системи управління безпечністю харчових продуктів має охоплювати:

а) задокументовані заяви про політику щодо безпечності харчових продуктів і відповідні цілі;

б) задокументовані процедури і протоколи відповідно до вимог ДСТУ ISO 22000;

в) документи, потрібні організації, щоб забезпечити результативне розроблення, запровадження і оновлення системи управління безпечністю харчових продуктів.

4.4.2.2 Керування документами

Необхідно керувати документами системи управління безпечністю харчових продуктів. Протоколи — особливий тип документів, і ними треба керувати відповідно до вимог, наведених у пп. 4.4.2.3.

Керування має забезпечувати, щоб всі запропоновані зміни було проаналізовано до їх упровадження, щоб установити їх наслідки для безпечності харчових продуктів і вплив на систему управління безпечністю харчових продуктів.

Потрібно встановити задокументовану процедуру для визначення елементів керування, необхідних для такого:

а) затвердження документів як відповідних до видання;

б) аналізування і, за потреби, актуалізування документів і повторного їх затвердження;

в) забезпечення ідентифікації змін і поточного статусу перегляду документів;

г) забезпечення наявності відповідних версій чинних документів у місцях їх застосування;

д) забезпечення розбірливості й простоти ідентифікації документів;

е) забезпечення ідентифікації документів зовнішнього походження та керування їх розповсюдженням;

ж) запобігання ненавмисному використанню застарілих документів і забезпечення їх належної ідентифікації в разі їх зберігання для будь-яких цілей.

4.4.2.3 Керування протоколами

Потрібно встановити і підтримувати протоколи для надання доказів відповідності вимогам і результативності системи управління безпечністю харчових продуктів. Протоколи мають бути доступними, розбірливими, легко ідентифікованими. Треба встановити задокументовану процедуру для визначення елементів керування, необхідних для ідентифікації, збереження, захисту, забезпечення доступу, дотримання строків зберігання і вилучення протоколів.

4.5 Відповідальність керівництва

4.5.1 Зобов'язання керівництва

Найвище керівництво має надавати докази виконання своїх зобов'язань щодо розроблення та запровадження системи управління безпечністю харчових продуктів і постійного поліпшування її результативності через такі дії:

а) демонстрування того, що безпечність харчових продуктів підтримується бізнесовими цілями організації;

б) інформування організації про важливість виконання вимог цього стандарту, законодавчих та інших нормативно-правових вимог, а також вимог замовників щодо безпечності харчових продуктів;

в) установлення політики щодо безпечності харчових продуктів;

г) аналізування з боку керівництва;

д) забезпечення наявності ресурсів.

4.5.2 Політика щодо безпечності харчових продуктів

Найвище керівництво має визначати, документувати і повідомляти свою політику щодо безпечності харчових продуктів.

Найвище керівництво має гарантувати, що політика щодо безпечності харчових продуктів є такою:

а) відповідною ролі організації в харчовому ланцюзі;

б) відповідною як законодавчим і нормативним вимогам, так і взаємоузгодженим вимогам замовників до безпечності харчових продуктів;

в) повідомленою, запровадженою та підтриманою на всіх рівнях організації;

г) аналізованою для постійної придатності;

д) адекватно спрямованою на інформування;

е) підтриманою вимірними цілями.

Приклад політики щодо безпечності харчових продуктів наведено у додатку Б.

4.5.3 Планування системи управління безпечністю харчових продуктів

Найвище керівництво має забезпечити проведення таких дій:

а) планування системи управління безпечністю харчових продуктів для виконання загальних вимог щодо системи управління безпечністю харчових продуктів, а також для досягнення цілей організації, які підтримують безпечність харчових продуктів;

б) підтримання цілісності системи управління безпечністю харчових продуктів під час планування і впровадження змін до цієї системи.

4.5.4 Відповідальність і повноваження

Найвище керівництво має забезпечити визначення відповідальності й повноважень та інформувати про це в межах організації для гарантування результативного функціювання й підтримування системи управління безпечністю харчових продуктів.

На весь персонал має бути покладено обов'язок повідомляти про проблеми в системі управління безпечністю харчових продуктів певній(им) особі(ам). Треба визначити призначеному персоналу відповідальність і надати повноваження для ініціювання та протоколювання дій.

4.5.5 Керівник групи управління безпечністю харчових продуктів

Найвищому керівництву слід призначити керівника групи управління безпечністю харчових продуктів, який незалежно від інших обов'язків має бути відповідальним і повноважним, щоб виконувати такі дії:

а) керувати группою управління безпечністю харчових продуктів й організовувати її роботу;

б) забезпечувати відповідну підготовленість та освіту учасників цієї групи;

в) забезпечувати встановлення, впровадження, підтримування і оновлювання системи управління безпечністю харчових продуктів;

г) звітувати перед найвищим керівництвом про результативність і придатність цієї системи.

Примітка. Обов'язки керівника цієї групи можуть охоплювати взаємодію із зовнішніми сторонами з питань, що стосуються системи управління безпечністю харчових продуктів.

4.5.6 Інформування

4.5.6.1 Зовнішнє інформування

Для забезпечення наявності у всьому харчовому ланцюзі достатньої інформації з питань щодо безпечності харчових продуктів в організації слід установити, впровадити і підтримати результативні заходи з інформування:

а) постачальників і підрядників;

б) замовників і споживачів, зокрема, стосовно інформації про продукт (охоплюючи інструкції щодо використання за призначеністю, конкретні вимоги до зберігання і, якщо доречно, термін придатності), запитів, контрактів або результатів опрацювання замовлень, враховуючи зміни та зворотний зв'язок із замовником, беручи до уваги його скарги;

в) законодавчих і регулятивних органів влади;

г) керівництва та співробітників інших організацій, що мають вплив або відчуватимуть вплив результативності або оновлення системи управління безпечністю харчових продуктів.

Такий процес інформування має забезпечувати надання інформації про аспекти безпечності харчових продуктів певної організації іншим організаціям харчового ланцюга. Це особливо стосується відомих небезпечних чинників харчових продуктів, якими мають керувати інші організації харчового ланцюга. Протоколи щодо інформування необхідно підтримувати у належному стані.

Мають бути наявними вимоги законодавчих і регулятивних органів влади і замовників щодо безпечності харчових продуктів.

Необхідно визначати призначеному персоналу відповідальність і надавати повноваження здійснювати зовнішнє інформування щодо безпечності харчових продуктів. Інформацію, отриману із зовнішніх джерел, потрібно долучати до вхідних даних оновлення системи і аналізування її з боку керівництва.

4.5.6.2 Внутрішнє інформування

Керівництво організації має встановлювати, впроваджувати і підтримувати результативні заходи з інформування персоналу щодо питань, вирішення яких впливає на безпечність харчових продуктів.

Для підтримування результативності системи управління безпечністю харчових продуктів в організації слід забезпечувати своєчасне інформування групи управління безпечністю харчових продуктів про такі зміни (але не обмежуючись тільки ними):

а) продуктів, які виготовляються в організації, або нових продуктів;

б) сировини, інгредієнтів і послуг;

в) виробничих приміщень, розташування устаткування, навколишнього середовища;

г) програми миття і дезінфікування;

д) пакування, зберігання та системи розподілювання (дистриб'юції);

е) рівнів кваліфікації персоналу та/або розподілу відповідальності й повноважень;

ж) законодавчих і нормативних вимог;

з) знань щодо небезпечних чинників харчових продуктів і заходів керування;

і) вимог замовника, галузевих та інших вимог, яких дотримується організація;

к) доречних запитів від зацікавлених зовнішніх сторін;

л) скарг, що вказують на небезпечні чинники харчових продуктів, що пов'язані з якістю цих продуктів;

м) інших умов, що впливають на безпечність харчових продуктів.

Група управління безпечністю харчових продуктів має забезпечувати враховування цієї інформації під час оновлювання системи управління безпечністю харчових продуктів. Найвищому керівництву слід забезпечувати внесення відповідної інформації до вхідних даних аналізування системи з боку керівництва.

4.5.7 Готовність до надзвичайних ситуацій і реагування на них

Найвище керівництво має встановлювати, впроваджувати і підтримувати процедури керування потенційними надзвичайними ситуаціями і аваріями, що можуть впливати на безпечність харчових продуктів, та які є доречними щодо ролі організації в харчовому ланцюзі.

4.5.8 Аналізування з боку керівництва

4.5.8.1 Загальні положення

Найвище керівництво має аналізувати систему управління безпечністю харчових продуктів організації із запланованою періодичністю для забезпечення її постійної придатності, адекватності та результативності. Таке аналізування має охоплювати оцінювання можливостей поліпшування системи управління безпечністю харчових продуктів і визначення потреби у її змінах, зокрема політики щодо безпечності харчових продуктів. Необхідно вести протоколи аналізування з боку керівництва.

4.5.8.2 Вхідні дані аналізування

У вхідних даних аналізування з боку керівництва має бути (без обмежень зазначеного) інформація щодо такого:

а) дій за результатами попередніх аналізувань з боку керівництва;

б) аналізування результатів дій стосовно перевіряння;

в) змінювання обставин, що можуть вплинути на безпечність харчових продуктів;

г) надзвичайних ситуацій, аварій і вилучень;

д) результатів аналізування дій стосовно оновлення системи;

е) аналізування дій стосовно інформування, зокрема зворотного зв'язку із замовником;

ж) зовнішніх аудитів або інспекцій.

Дані треба подавати так, щоб найвище керівництво мало змогу пов'язати інформацію із заявленими цілями, що стосуються системи управління безпечністю харчових продуктів.

4.5.8.3 Вихідні дані аналізування

У вихідних даних аналізування з боку керівництва мають бути зазначені рішення та дії, пов'язані з таким:

а) убезпеченням харчових продуктів;

б) підвищенням результативності системи управління безпечністю харчових продуктів;

в) потребами у ресурсах;

г) переглядом політики організації щодо безпечності харчових продуктів і пов'язаних з цим цілей.

4.6 Управління ресурсами

4.6.1 Забезпечення ресурсами

Керівництво організації має забезпечити наявність відповідних ресурсів для встановлення, запровадження, підтримування і оновлення системи управління безпечністю харчових продуктів.

4.6.2 Людські ресурси

4.6.2.1 Загальні положення

Група управління безпечністю харчових продуктів та інший персонал, який виконує роботу, що впливає на безпечність харчових продуктів, повинен бути компетентним і мати належну освіту, підготовленість, кваліфікацію та досвід.

Якщо для розроблення, запровадження, функціювання або оцінювання системи управління безпечністю харчових продуктів потрібна допомога зовнішніх експертів, мають бути наявними письмові угоди або контракти, що визначають відповідальність і повноваження зовнішніх експертів.

4.6.2.2 Компетентність, обізнаність і навчання

В організації мають виконуватися такі дії:

а) визначати необхідний рівень компетентності персоналу, чия діяльність впливає на безпечність харчових продуктів;

б) організовувати навчання або виконувати інші дії для забезпечення необхідного рівня компетентності персоналу;

в) забезпечувати належну підготовленість персоналу, відповідального за моніторинг, коригування та коригувальні дії в межах системи управління безпечністю харчових продуктів;

г) оцінювати запровадження та результативність описаних дій (див. а, б, в);

д) забезпечувати обізнаність персоналу щодо доречності та важливості внеску своєї індивідуальної діяльності для убезпечення харчових продуктів;

е) забезпечувати, щоб вимога щодо результативного інформування була зрозумілою всьому персоналу, чия діяльність впливає на безпечність харчових продуктів;

ж) вести відповідні протоколи щодо навчання та зазначених дій (див. б, в).

4.6.3 Інфраструктура

Керівництву організації слід забезпечити ресурси для створення та підтримування інфраструктури, необхідної для задоволення вимог цього стандарту.

4.6.4 Робоче середовище

Керівництву організації слід забезпечити ресурси для створення, управління та підтримування робочого середовища, необхідного для задоволення вимог цього стандарту.

4.7 Планування і випуск безпечної продукції

4.7.1 Загальні положення

В організації слід планувати й розробляти процеси, необхідні для випуску безпечних продуктів.

Керівництву організації слід забезпечувати впровадження і виконання запланованих дій, їх результативність і будь-які їх зміни. Це охоплює ПП, а також операційні ПП і / або план НАССР.

4.7.2 Програми-передумови

4.7.2.1 В організації необхідно встановлювати, впроваджувати і підтримувати ПП для сприяння керуванню:

а) ймовірністю потрапляння небезпечного чинника до харчового продукту через робоче середовище;

б) біологічним, хімічним і фізичним забрудненням продукту(-ів), зокрема перехресним забрудненням між продуктами;

в) рівнями небезпечного чинника в харчовому продукті та середовищі, в якому його виготовляють.

4.7.2.2 ПП мають бути такими:

а) відповідати потребам організації щодо безпечності харчових продуктів,

в) відповідати розміру і типу виробництва, а також характеру продукції, яку виготовляють і / або обробляють;

г) запровадженими у всій системі виробництва або як програми загального застосування, або як програми, застосовувані щодо окремого продукту або виробничої лінії;

д) схваленими группою управління безпечністю харчових продуктів.

В організації слід визначати законодавчі та нормативні вимоги, що стосуються наведеного вище.

4.7.2.3 Вибираючи та / або встановлюючи ПП, необхідно брати до уваги та використовувати відповідну інформацію (наприклад, законодавчі й нормативні вимоги, вимоги замовників, визнані настанови, принципи і кодекси Комісії Codex Alimentarius (Codex), національні, міжнародні й галузеві стандарти).

Установлюючи такі програми, слід брати до уваги:

а) конструкцію і план будівель і пов’язаних з ними інженерних комунікацій;

б) план приміщень з робочими зонами та побутовими приміщеннями;

в) системи постачання повітря, води, електроенергії та інші інженерні комунікації;

г) допоміжні служби, зокрема утилізацію відходів і стічних вод;

д) придатність устаткування та його доступність для миття, технічного обслуговування й профілактичного ремонту;

е) керування закупленими матеріалами (наприклад, сировиною, інгредієнтами, хімічними речовинами, пакувальними матеріалами), постачанням (наприклад, води, повітря, пари і льоду), утилізацією (наприклад, відходів і стічних вод) та оперуванням продуктами (наприклад, їх зберіганням і транспортуванням);

ж) заходи щодо запобігання перехресному забрудненню;

з) миття та дезінфекцію;

і) контроль шкідників;

к) гігієну персоналу;

л) інші відповідні аспекти.

Необхідно планувати перевіряння ПП і модифікувати їх у разі необхідності.

Потрібно вести протоколи перевіряння та модифікації.

У документах має бути визначено, як керують діями, внесеними до ПП.

4.7.3 Попередні кроки, щоб уможливити аналізування небезпечних чинників

4.7.3.1 Загальні положення

Всю доречну інформацію, яка необхідна для виконання аналізу небезпечних чинників, потрібно збирати, підтримувати, оновлювати та документувати. Необхідно вести протоколи.

4.7.3.2 Група управління безпечністю харчових продуктів

Потрібно призначити групу управління безпечністю харчових продуктів.

Група безпечності харчових продуктів повинна мати багатодисциплінарні знання і досвід розроблення й запровадження систем управління безпечністю харчових продуктів. Такі знання стосуються продуктів організації, процесів, устаткування та небезпечних чинників харчових продуктів у межах сфери застосування системи управління безпечністю харчових продуктів, але не обмежуються ними.

Потрібно вести протоколи для демонстрування того, що члени групи управління безпечністю харчових продуктів мають необхідні знання і досвід.

4.7.3.3 Характеристики продукту

4.7.3.3.1 Сировина, інгредієнти і матеріали, що контактують з продуктом

Усю сировину, інгредієнти і матеріали, що контактують з продуктом, потрібно описувати в документах настільки докладно, наскільки це необхідно для аналізування небезпечних чинників, охоплюючи, коли доречно, таке:

а) біологічні, хімічні й фізичні характеристики;

б) склад багатоскладникових інгредієнтів з домішками й допоміжними матеріалами;

в) походження;

г) спосіб виробництва;

д) методи пакування і постачання;

е) умови зберігання і строк придатності;

ж) підготування і / або оперування перед використанням або обробленням;

з) пов’язані з безпечністю харчових продуктів критерії прийнятності або специфікації закуповуваних матеріалів та інгредієнтів, а також з їх використанням за призначенням.

В організації слід визначати законодавчі й нормативні вимоги до безпечності харчових продуктів, що стосуються наведеного вище.

Записи необхідно складати на основі актуальних даних (див. у п. 4.7.7).

4.7.3.3.2 Характеристика кінцевих продуктів

Характеристики кінцевих продуктів потрібно навести в документах настільки докладно, наскільки це необхідно для аналізування небезпечних чинників із застосуванням, коли доречно, такої інформації:

а) назви продукту або подібної ідентифікації;

б) складу;

в) біологічних, хімічних і фізичних характеристик, які стосуються безпечності харчових продуктів;

г) визначених строку придатності й умов зберігання;

д) пакування;

е) маркування стосовно безпечності харчових продуктів і / або інструкції щодо оперування, приготування та використання;

ж) методів розподіляння.

В організації мають визначати законодавчі й нормативні вимоги до безпечності харчових продуктів, що стосуються наведеного вище.

Записи необхідно складати на основі актуальних даних (див. у п. 4.7.7).

4.7.3.4 Використання за призначеністю

Використання за призначенням, обґрунтовано очікуване оперування кінцевим продуктом і будь-яке ненавмисне, але обґрунтовано очікуване неналежне оперування та неправильне використання кінцевого продукту має бути враховано і описано в документах настільки докладно, наскільки це необхідно для аналізування небезпечних чинників.

Для кожного продукту необхідно визначати групи споживачів і враховувати групи споживачів, відомі як особливо вразливі до конкретних небезпечних чинників харчових продуктів.

Записи необхідно складати на основі актуальних даних (див. у п. 4.7.7).

4.7.3.5 Блок-схеми процесу, стадії процесу і заходи керування

4.7.3.5.1 Блок-схеми процесу

Блок-схеми процесу мають бути підготовленими для категорій продуктів або процесів, які охоплені системою управління безпечністю харчових продуктів. Блок-схеми мають бути основою для оцінювання можливої появи, збільшення або внесення небезпечних чинників до харчових продуктів.

Блок-схеми процесів мають бути чіткими, точними і достатньо деталізованими. У блок-схемах потрібно, коли доречно, вказувати таке:

а) послідовність і взаємодію всіх стадій процесу;

б) будь-які процеси, що виконують за межами організації, та субпідрядні роботи;

в) стадії, де сировину, інгредієнти і проміжні продукти вводять у процес;

г) стадії, де відбувається перероблення та повторне використання продуктів;

д) стадії, де кінцеві, проміжні, побічні продукти і відходи випускають або вилучають.

Група управління безпечністю харчових продуктів має перевіряти точність блок-схем процесів контролем на місці. Перевірені блок-схеми слід оформлювати і зберігати як протоколи.

4.7.3.5.2 Опис стадій процесу і заходів керування

Заходи керування, параметри процесів і відповідне їх застосування або процедури, які можуть впливати на безпечність харчових продуктів, потрібно описувати настільки докладно, наскільки це необхідно для аналізування небезпечних чинників.

Слід також описувати зовнішні вимоги (наприклад, регулятивних органів або замовників), що можуть впливати на вибір і відповідне використання заходів керування.

Записи потрібно оновлювати відповідно до п. 4.7.7.

4.7.4 Аналізування небезпечних чинників

4.7.4.1 Загальні положення

Група управління безпечністю харчових продуктів має аналізувати небезпечні чинники, щоб установлювати, якими саме небезпечними чинниками слід керувати, який ступінь керування є потрібним для убезпечення харчових продуктів і яка комбінація заходів керування є необхідною.

4.7.4.2.1 Усі небезпечні чинники харчових продуктів, виникнення яких є обґрунтовано очікуваним, зважаючи на тип продукту, тип процесу і наявну виробничу інфраструктуру, потрібно ідентифікувати та протоколювати. Ідентифікацію треба базувати на такому:

а) попередній інформації і даних, зібраних відповідно до п. 4.7.3;

б) досвіді;

в) зовнішній інформації, зокрема, наскільки це можливо, епідеміологічних та інших історичних даних;

г) отриманій з харчового ланцюга інформації щодо небезпечних чинників харчових продуктів, які можуть стосуватися безпечності кінцевих, проміжних і харчових продуктів під час споживання.

Стадію(-ї) (від сировини до оброблення та розподіляння), на якій(-их) може бути внесено кожний небезпечний чинник харчового продукту, потрібно позначати.

4.7.4.2.2 Ідентифікуючи небезпечні чинники, треба брати до уваги таке:

а) стадії, що передують розглядуваній операції, та наступні за нею;

б) технологічне устаткування, допоміжні служби обслуговування і оточення;

в) попередні й подальші ланки харчового ланцюга.

4.7.4.2.3 Якщо це можливо, для кожного ідентифікованого небезпечного чинника потрібно визначати його прийнятний рівень у кінцевому продукті. Треба, щоб у визначеному рівні було враховано чинні законодавчі та нормативні вимоги, вимоги замовника до безпечності харчового продукту, використання продукту за призначеністю замовником та інші доречні дані. Обґрунтування і результат визначення прийнятних рівнів потрібно запротоколювати.

4.7.4.3 Оцінювання небезпечних чинників

Оцінювання небезпечних чинників слід проводити, щоб установити, чи є усунення або зменшення до прийнятних рівнів кожного небезпечного чинника суттєвим для виробництва безпечного харчового продукту, чи є необхідним керування ним, щоб уможливити дотримання визначених прийнятних рівнів.

Кожний небезпечний чинник потрібно оцінити стосовно можливих істотних негативних впливів на здоров’я людини і ймовірності їх виникнення.

Використовувану методологію потрібно описати, а результати оцінювання небезпечних чинників запротоколювати.

4.7.4.4 Вибирання і оцінювання заходів керування

Спираючись на оцінювання небезпечних чинників, треба вибрати відповідну комбінацію заходів керування, здатну запобігти впливу цих небезпечних чинників, або усунути чи зменшити його до встановлених прийнятних рівнів.

Під час цього вибору кожний захід керування потрібно аналізувати стосовно його результативності щодо ідентифікованих небезпечних чинників харчового продукту. Вибрані заходи керування мають бути розподілені за категоріями стосовно потреби їх виконання за допомогою операційної(-их) ПП або плану НАССР.

Вибирання і розподіляння заходів керування за категоріями треба провадити, використовуючи логічний підхід, що містить оцінювання з урахуванням такого:

а) впливу заходу керування на ідентифікований небезпечний чинник стосовно відповідповідності застосування;

б) здійсненності моніторингу заходу керування (наприклад, спроможності вчасно провести моніторинг задля визначення можливості негайного коригування);

в) місця вибраного заходу керування у системі відносно інших заходів керування;

г) імовірності порушення функціювання заходу керування або істотної мінливості процесу;

д) істотності наслідка(ів) у разі порушення функціювання заходу керування;

е) чи є захід керування спеціально розробленим і застосованим для усунення або суттєвого зменшення рівня небезпечного(их) чинника(ів);

ж) синергетичних ефектів (тобто взаємодії, яка виникає між двома або кількома заходами і призводить до того, що їхній сукупний вплив вищий, ніж сума впливів кожного з них).

Заходи керування, що належать до плану HACCP, потрібно виконувати відповідно до п. 4.7.6, а інші заходи керування – як операційні ПП відповідно до п. 4.7.5.

Методологію і параметри, використані для цього розподілу за категоріями, слід описати в документах, а результати оцінювання — запротоколювати.

4.7.5 Установлення операційних програм-передумов

Операційні ПП треба задокументувати, в них має бути така інформація щодо кожної програми:

а) небезпечний(і) чинник(и) харчових продуктів, який(і) слід скеровувати програмою;

б) захід(оди) керування;

в) процедури моніторингу для демонстрування того, що операційні ПП упроваджено;

г) коригування і коригувальні дії, які необхідно виконувати в разі, коли моніторинг свідчитиме про відсутність керування операційними ПП;

д) відповідальність і повноваження;

е) протокол(и) моніторингу.

4.7.6 Установлення плану HACCP

4.7.6.1 План HACCP

План HACCP треба задокументувати, в ньому має бути така інформація щодо кожної ідентифікованої критичної точки керування (КТК):

а) небезпечний(і) чинник(и) харчових продуктів, яким(и) керують у КТК;

б) захід(оди) керування;

в) критична(і) межа(і);

г) процедура(и) моніторингу;

д) коригування і коригувальні дії, які необхідно виконати в разі порушення критичних меж;

е) відповідальність і повноваження;

ж) протокол(и) моніторингу.

4.7.6.2 Ідентифікація КТК

Для кожного небезпечного чинника під керуванням плану HACCP потрібно ідентифікувати КТК відповідно до встановленних заходів керування.

4.7.6.3 Визначення критичних меж для КТК

Для моніторингу, встановленого для кожної КТК, потрібно визначити критичні межі.

Критичні межі необхідно встановити для забезпечення того, що ідентифікований прийнятний рівень небезпечного чинника в кінцевому продукті не буде перевищено.

Критичні межі мають бути вимірними.

Обґрунтування вибраних критичних меж треба задокументувати.

Визначення критичних меж на основі суб'єктивних даних (зокрема візуальної перевірки продукту, процесу тощо) слід виконувати відповідно до інструкцій або специфікацій і з урахуванням компетентності співробітників.

4.7.6.4 Система моніторингу КТК

Для кожної КТК треба встановлювати систему моніторингу для демонстрування того, що КТК знаходиться під контролем. У систему входять усі заплановані вимірювання або спостереження, що стосуються критичних(ої) меж(і).

У системі моніторингу мають бути відповідні процедури, інструкції та протоколи, за допомогою яких описують таке:

а) вимірювання або спостереження, в результаті яких одержують дані в часових межах;

б) прилади, використовувані для моніторингу;

в) застосовувані методи калібрування;

г) періодичність моніторингу;

д) відповідальність і повноваження, пов'язані з моніторингом та оцінюванням його результатів;

е) вимоги до протоколів і методи їх ведення.

Визначені в організації методи і періодичність моніторингу мають забезпечувати своєчасне встановлення перевищення критичних меж, щоб ізолювати продукт перш ніж його буде використано або спожито.

4.7.6.5 Дії в разі, коли результати моніторингу перевищують критичні межі

Заплановані коригування і коригувальні дії, які необхідно виконувати в разі перевищення критичних меж, потрібно зазначити в плані НАССР. Ці дії мають бути спрямовані на виявлення причини невідповідності задля забезпечення керування та запобігання повторювання невідповідності.

Необхідно встановлювати й підтримувати задокументовані процедури належного контролю потенційно небезпечними продуктами, щоб гарантувати, що їх не буде випущено, поки не буде оцінено.

4.7.7 Оновлення попередньої інформації й документів, які визначають ПП і план НАССР

Після встановлення операційних ПП і / або плану НАССР в організації має бути оновлена, за потреби, така інформація:

а) характеристики продукту;

б) опис його використання за призначенням;

в) блок-схеми процесу;

г) стадії процесу;

е) заходи керування.

У разі необхідності план НАССР, процедури та інструкції, що визначають ПП, потрібно виправляти.

4.7.8 Планування перевіряння

Планування перевіряння має визначати мету, методи, періодичність і відповідальність щодо дій з перевіряння. Ці дії мають підтверджувати таке:

а) ПП впроваджено;

б) вхідні дані для аналізування небезпечних чинників постійно оновлюють;

в) операційні ПП і елементи плану НАССР впроваджено, і вони є результативними;

г) рівні небезпечних чинників знаходяться у межах визначених прийнятних рівнів;

д) інші процедури, що є необхідними організації, впроваджено, і вони — результативні.

Вихідні дані такого планування повинні мати форму, відповідну методам функціювання організації.

Результати перевірення потрібно протоколювати і повідомляти групі управління безпечністю харчових продуктів. Ці результати слід подавати своєчасно, щоб уможливити аналізування результатів дій з перевіряння.

Якщо в основі перевіряння системи лежить випробування зразків кінцевого продукту і коли під час його проведення випробні зразки демонструють невідповідність прийнятному рівню небезпечного чинника харчового продукту, то ушкоджені партії продукції слід визнавати як потенційно небезпечні.

4.7.9 Система простежуваності

В організації слід встановлювати і застосовувати систему простежуваності, яка дає змогу ідентифікувати партії продукції та їх зв'язок з партіями сировини, протоколами щодо оброблення і постачання.

Система простежуваності має бути придатною ідентифікувати матеріали, що надходять від безпосереднього постачальника, та початковий маршрут розподіляння кінцевого продукту.

Протоколи простежуваності потрібно зберігати протягом визначеного періоду для оцінювання системи, щоб уможливити управління потенційно небезпечними продуктами та на випадок вилучення продукції. Протоколи мають відповідати законодавчим і нормативним вимогам і вимогам замовників і можуть, наприклад, містити ідентифікацію партії кінцевого продукту.

4.7.10 Керування невідповідністю

4.7.10.1 Коригування

В організації слід забезпечувати, щоб у разі перевищення критичних меж КТК або втрати керування операційними ПП, продукти, які зазнали негативного впливу, було ідентифіковано та ними керували з урахуванням їх використання і випуску.

Потрібно встановлювати й підтримувати задокументовану процедуру, що визначає таке:

а) ідентифікування і оцінювання ушкоджених кінцевих продуктів для встановлення належного управління ними;

б) аналізування виконаних коригувань.

Продукти, вироблені в умовах перевищення критичних меж, є потенційно небезпечними і оперувати ними слід згідно з пп. 4.7.10.3. Продукти, вироблені в умовах відсутності відповідності операційним ПП, мають бути оцінені стосовно причин(и) невідповідності і наслідків щодо безпечності і, за потреби, оперувати ними слід відповідно до пп. 4.7.10.3. Результати оцінювання потрібно запротоколювати.

Усі дії, щодо коригування продукції має(ють) схвалити відповідальна(і) особа(и), і їх слід запротоколювати разом з інформацією про характер невідповідності, її причину(и) і наслідки, зокрема з інформацією, необхідною для досягнення цілей простежуваності невідповідних партій.

4.7.10.2 Коригувальні дії

Дані, отримані за результатами моніторингу операційних ПП і КТК, має оцінювати уповноважена(-і) особа(-и), що має(-ють) достатні знання і повноваження для ініціювання коригувальних дій.

Коригувальні дії потрібно ініціювати в разі перевищення критичних меж або коли бракує відповідності даних операційним ПП.

В організації слід розробити і підтримувати задокументовані процедури, які визначають належні дії для ідентифікування і усунення причин виявлених невідповідностей для запобігання їх повторному виникненню й повернення процесу або системи під керування.

Такі дії містять:

а) аналізування невідповідностей (зокрема скарг замовників);

б) аналізування тенденцій результатів моніторингу, які можуть указувати на можливість утрати керування;

в) визначення причин(и) невідповідностей;

г) оцінювання потреби в діях, які б забезпечували запобігання повторенню невідповідності;

д) визначення та застосовування потрібних дій;

е) протоколювання результатів виконаних коригувальних дій;

ж) аналізування виконаних коригувальних дій для забезпечення їх результативності.

Результати виконання коригувальних дій слід протоколювати.

4.7.10.3 Оперування потенційно небезпечними продуктами

4.7.10.3.1 Загальні положення

В організації слід управляти невідповідними продуктами через здійснення заходів щодо запобігання потраплянню такої продукції до харчового ланцюга, якщо неможливо гарантувати такі дії:

а) небезпечні чинники харчових продуктів, що спричиняють занепокоєння, зменшено до визначених прийнятних рівнів;

б) небезпечні чинники харчових продуктів, які спричиняють занепокоєння, буде зменшено до визначених прийнятних рівнів перш ніж продукт потрапить до харчового ланцюга;

в) продукт і далі відповідатиме визначеному(им) прийнятному(им) рівню(ям) небезпечного(их) чинника(ів), незважаючи на невідповідність.

Усі партії продукту, на які могла вплинути небезпечна ситуація, потрібно утримувати під контролем організації, доки не буде оцінено їхній рівень безпечності.

Якщо продукти, які вийшли з-під контролю організації, у подальшому визнано небезпечними, керівництво організації має повідомити про це відповідні зацікавлені сторони та ініціювати вилучення цих продуктів.

Елементи керування, відповідне реагування і повноваження щодо роботи з потенційно небезпечними продуктами потрібно задокументувати.

4.7.10.3.2 Оцінювання продуктів для випуску

Кожну партію продукції, виробленої в умовах невідповідності, слід випускати як безпечну тільки тоді, коли виконано одну з таких умов:

а) наявність інших доказів чим ті, що подає система моніторингу, які підтверджують, що заходи керування були результативними;

б) докази свідчать, що сукупний вплив заходів керування на конкретний продукт відповідає призначеній результативності (тобто прийнятним рівням небезпечних чинників харчових продуктів (див. пп. 4.7.4.2);

в) результати вибіркових випробувань, аналізування та / або інших дій з перевіряння свідчать, що ушкоджена партія продукції задовольняє визначеним прийнятним рівням небезпечних чинників харчових продуктів.

4.7.10.3.3 Розміщування невідповідного продукту

Якщо за результатами оцінювання партія продукції не є прийнятною для випускання, то слід виконувати одну з таких дій:

а) піддавати переробленню або продовжувати оброблення в межах організації або поза ними для забезпечення того, щоб небезпечний чинник харчового продукту було усунено або зменшено до прийнятного рівня;

б) знищувати або утилізувати як відходи.

4.7.10.4 Вилучення

Щоб уможливити і полегшити цілковите і своєчасне вилучення партій кінцевих продуктів, які було ідентифіковано як небезпечні, слід виконувате таке:

а) найвищому керівництву необхідно призначати персонал, який матиме повноваження ініціювати вилучення, та персонал, який відповідатиме за виконання вилучення;

б) в організації слід встановлювати й підтримувати задокументовану процедуру щодо такого:

1) сповіщання відповідних зацікавлених сторін (наприклад, законодавчих і регулятивних органів, замовників і / або споживачів);

2) управління вилученими продуктами, а також ушкодженими партіями продукції, які ще перебувають на складі;

3) послідовності дій, які потрібно виконати.

Вилучені продукти потрібно охороняти або утримувати під наглядом, доки їх не буде знищено, використано для цілей, відмінних від початкової призначеності, визнано безпечними для того самого (або іншо-

го) використання за призначеністю або перероблено у спосіб, що гарантує їх безпечність.

Причину, ступінь і результат вилучення потрібно протоколювати і повідомляти найвищому керівництву як вхідні дані для аналізування з боку керівництва (див. пп. 4.5.8.2).

Співробітники організації мають перевіряти і протоколювати результативність програми вилучення через застосування відповідних методів (наприклад, удаване вилучення або практичне вилучення).

4.8 Підтвердження, перевіряння і поліпшування системи управління безпечністю харчових продуктів

4.8.1 Загальні положення

Група управління безпечністю харчових продуктів має планувати і впроваджувати процеси, необхідні для підтвердження заходів керування та / або їх комбінацій, перевіряння і поліпшування системи управління безпечністю харчових продуктів.

4.8.2 Підтвердження комбінацій заходів керування

До впровадження заходів керування, які буде долучено до операційних ПП і плану HACCP, і після внесення будь-яких змін до них керівництво організації має підтвердити таке:

а) спроможність вибраних заходів керування сприяти досягненню призначеного рівня керування небезпечним(и) чинником(ами) харчових продуктів, для яких їх розроблено;

б) результативність заходів керування і спроможність їх комбінації забезпечити керування ідентифікованим(и) небезпечним(и) чинником(ами) харчових продуктів для одержання кінцевого продукту, що відповідає визначеним прийнятним рівням.

Якщо результат підтвердження свідчить про те, що одну або обидві з наведених вище вимог не можна підтвердити, то заходи керування та / або їх комбінацію треба змінити й повторно провести оцінювання.

Модифікації можуть охоплювати змінення заходів керування (тобто параметрів процесу, суворості та / або їх комбінацію) сировиною, технологіями виробництва, характеристиками кінцевого продукту, методами розподілення, а також змінення щодо використання за призначеністю кінцевого продукту.

4.8.3 Керування моніторингом і вимірюванням

Співробітники організації мають надати докази того, що визначені методи й устаткування для проведення моніторингу і вимірювань є адекватними для того, щоб забезпечувати виконання цих процедур.

Коли необхідно забезпечувати вірогідність результатів, користування вимірювальним устаткуванням і застосування визначених методів, слід виконувати такі дії:

а) калібрувати або перевіряти їх з визначеною періодичністю або перед використанням згідно з міжнародними або національними еталонами, якщо таких еталонів немає, потрібно запротоколювати базу для калібрування або перевіряння;

б) настроювати або, за потреби, повторно настроювати;

в) ідентифікувати для уможливлення визначення статусу калібрування;

г) захищати від настроювань, що можуть спричинити невірогідність результатів вимірювання,

д) захищати від пошкодження і псування.

Необхідно зберігати записи про результати калібрування й перевіряння.

Якщо виявлено, що устаткування або процес не відповідають вимогам, в організації слід провести оцінювання вірогідності результатів попередніх вимірювань. Якщо устаткування для проведення вимірювань є невідповідним, необхідно застосовувати належні заходи щодо такого устаткування або будь-якого неадекватного продукту. Результати такого оцінювання і наступні дії потрібно запротоколювати.

Якщо для моніторингу і вимірювання окремих показників використовують комп'ютерне програмне забезпечення, його спроможність задовольняти призначене застосування необхідно підтвердити.

Підтвердження слід провести до першого використання та, за потреби, провадити повторно.

4.8.4 Перевіряння системи управління безпечністю харчових продуктів

4.8.4.1 Внутрішній аудит

В організації слід проводити внутрішні аудити із запланованою періодичністю для впевненості в тому, що система управління безпечністю харчових продуктів:

а) відповідає запланованим заходам, вимогам, установленим до неї в організації, та вимогам ДСТУ ISO 22000;

б) результативно запроваджена й оновлюється.

Програму аудиту слід планувати з урахуванням важливості процесів і ділянок, що підлягають аудиту, а також будь-яких дій з оновлення, виконаних за результатами попередніх аудитів. Потрібно визначити критерії аудиту, обсяг, періодичність і методи його проведення. Вибір аудиторів і проведення аудитів мають забезпечувати об'єктивність і не-

упередженість процесу аудиту. Аудитори не мають здійснювати аудит своєї роботи.

Відповідальність і вимоги щодо планування й виконання аудитів, звітування про їх результати і ведення протоколів потрібно визначити в задокументованій процедурі.

Керівництво, відповідальне за ділянку, аудит якої провадять, має забезпечити виконання дій з усунення виявлених невідповідностей та їх причин без зайвого затримання. У подальших заходах слід перевіряти виконані дії і звітувати про їх результати.

4.8.4.2 Оцінювання індивідуальних результатів перевіряння

Група управління безпечністю харчових продуктів має систематично оцінювати індивідуальні результати запланованого перевіряння.

Якщо результати перевіряння не свідчат про відповідність запланованим заходам, керівництву організації необхідно визначити і виконати дії для досягнення необхідної відповідності. Такі дії мають містити (але не обмежуватись тільки цим) аналіз такого:

а) наявних процедур і каналів інформування;

б) висновків розгляду небезпечних чинників, установлених операційних ПП і плану НАССР;

в) ПП;

г) результативності керування людськими ресурсами та діяльності щодо навчання.

Група управління безпечністю харчових продуктів має аналізувати результати перевірок, зокрема результати внутрішніх і зовнішніх аудитів. Аналізування потрібно проводити для виконання таких дій:

а) підтвердження того, що загальне функціонування системи управління безпечністю харчових продуктів відповідає запланованим заходам і вимогам, установленим в організації;

б) установлення потреби в оновленні або поліпшуванні цієї системи;

в) визначення тенденцій, що вказують на збільшення частки потенційно небезпечних харчових продуктів;

г) збирання інформації для планування програми внутрішнього аудиту стосовно статусу та важливості ділянок, які підлягають перевірці;

д) наведення доказів того, що всі виконані коригування і коригувальні дії є результативними.

Результати аналізування та пов’язані з ним заходи слід протоколювати й повідомляти найвищому керівництву як вхідні дані для аналізування з боку керівництва. Їх також потрібно використовувати як вхідні

дані для оновлення системи управління безпечністю харчових продуктів.

4.8.5 Поліпшування

4.8.5.1 Постійне поліпшування

Найвище керівництво має забезпечувати постійне поліпшення результативності системи управління безпечністю харчових продуктів, використовуючи процеси інформування, аналізування з боку керівництва, внутрішній аудит, оцінювання індивідуальних результатів перевірення, аналізування результатів дій з перевіряння, формування комбінацій щодо заходів керування, коригувальних дій і оновлення системи управління безпечністю харчових продуктів.

4.8.5.2 Оновлення системи управління безпечністю харчових продуктів

Найвище керівництво має забезпечувати постійне оновлювання системи управління безпечністю харчових продуктів.

Для досягнення цього групі управління безпечністю харчових продуктів слід оцінювати систему із запланованою періодичністю. Група має вирішати, чи потрібно переглядати процедуру аналізу небезпечних чинників, установлені операційні ПП і план НАССР.

Дії щодо оцінювання і оновлення системи мають бути основані на таких даних:

а) вхідних, отриманих внаслідок інформування як зовнішнього, так і внутрішнього;

б) вхідних стосовно іншої інформації щодо придатності, адекватності й результативності системи управління безпечністю харчових продуктів;

в) вихідних даних аналізування результатів перевірок;

г) вихідних даних аналізування з боку керівництва.

Результати дій стосовно оновлення системи потрібно протоколювати й повідомляти керівництву як вхідні дані для аналізування.

Контрольні запитання

1. Якою є сфера застосування ДСТУ ISO 22000?
2. Що таке небезпечні чинники харчової продукції?
3. Які дії необхідно впровадити для організації внутрішнього інформування?
4. Що містить план НАССР?
5. Що таке програма-передумова?
6. Які існують види характеристик харчового продукту?

БІБЛІОГРАФІЧНИЙ СПИСОК

1 Інтегрована система менеджменту [Електронний ресурс]. – Режим доступу або URb: https://uk.wikipedia.org/wiki/Інтегрована_система_менеджменту.

2 Інтегрована система менеджменту [Електронний ресурс]. – Режим доступу або URb:http://ua-referat.com/Інтегровані_системи_управління.

3 ДСТУ ISO 9001: 2009. Системи управління якістю. Вимоги. – К.: Держспоживстандарт України, 2009. – 30 с.

4 ДСТУ ISO 14001: 2004. Системи екологічного менеджменту. Вимоги. – К.: Держспоживстандарт України, 2004. – 20 с.

5 ДСТУ OHSAS 18001:2010. Система управління гігієною та безпекою праці. – К.: Держспоживстандарт України, 2010. – 20 с.

6 ДСТУ ISO/IEC 27001:2010. Інформаційні технології. Методи та засоби досягнення інформаційної безпеки. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, IDT). – К.: Держспоживстандарт України, 2010. – 25 с.

7 ДСТУ ISO 22000:2007. Системи управління безпечністю харчових продуктів. Вимоги до будь-яких організацій харчового ланцюга. – К.: Держспоживстандарт України, 2007. – 30 с.

8 ДСТУ ISO/CD 26000:2009. Системи управління соціальною відповідальністю. Вимоги. – К.: Держспоживстандарт України, 2007. – 130 с.

9 SA 8000 Social Accountability (Соціальна відповідальність) [Електронний ресурс]. – Режим доступу або URb: http://zakon3.rada.gov.ua/laws/show/n0015697-07.

10 ДСТУ ISO/IEC 17025:2006. Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій. – К.: Держспоживстандарт України, 2007. – 26 с.

11 ДСТУ ISO 50001:2014. Енергозбереження. Системи енергетичного менеджменту. Вимоги та настанова щодо використання (ISO 50001:2011, IDT). – К.: Держспоживстандарт України, 2007. – 27 с.

12 ISO 55001:2014. Asset management – Management systems – Requirements (Управління активами. Система управління. Вимоги). [Електронний ресурс]. – Режим доступу або URb: http://www.iso.org/iso/catalogue_detail?csnumber=55089.

13 ДСТУ-П IWA 2:2009. Системи управління якістю. Настанови щодо застосування ISO 9001:2000 у сфері освіти (IWA 2:2007, IDT). – К.: ДП «НДІ «Система», 2009. – 19 с.

14 Національний класифікатор України. Класифікація видів економічної діяльності КВЕД 009:2010. – К.: Держспоживстандарт України, 2012. – 45 с.

15 Шаповал, М. І. Менеджмент якості [Текст]: підручник / М. І. Шаповал. – К.: Знання, 2003. – 475 с.

16 Трофимов, К. Б. Процесний підхід при організації системи управління якістю [Текст]: метод. рекомендації / К. Б.Трофимов, Н. В. Чернобай. – Х.: Нац. аерокосм. ун-т «ХАІ», 2007. – 31 с.

17 Трофимов, К. Б. Методика аудита систем управления качеством [Тескт]: учеб. пособие / К. Б. Трофимов. – Х.: Нац. аэрокосм. ун-т «ХАИ», 2004. – 82 с.

18 Система качества по МС ИСО серии 9000. Политика предприятия в области качества: брошюры. – СПб. : ИЦ «Аргус-Стандарт», 1992. – 57 с.

19 Никитин, В .А. Управление качеством на базе стандартов ИСО 9000:2000 [Текст] / В. А. Никитин. – СПб.: Питер, 2004. – 157 с.

20 Никитин, В. А. Управление качеством на базе стандартов ИСО 9000:2000 [Текст] / В. А. Никитин, В. В. Филончева. – 2-е изд. – СПб. : Питер, 2004. – 93 с.

21 Орлов, П. А. Менеджмент качества и сертификация продукции [Текст]: учеб. пособие / П. А. Орлов. – Х.: Издательский дом "ИНЖЭК", 2004. – 304 с.

22 Літвак, С.М. Екологічний менеджмент і аудит [Текст]: навч. посібник / С. М. Літвак. – К.: Професіонал, 2005. – 112 с.

23 Політика ПрАТ «УКРСТАЛЬКОНСТРУКЦІЯ» [Електронний ресурс]. – Режим доступу або URb: http://www.steelwork.com.ua/ru/home/aboutus/politics.html.

24 Политика ВАТ «Запорожсталь» [Електронний ресурс]. – Режим доступа или URb: http://www.zaporizhstal.com/media/cms_page_media/105/Politika_2.jpg.

25 Політика підприємства в питаннях якості та безпечності продуктів харчування, охорони навколишнього середовища, охорони праці та здоров'я [Електронний ресурс]. – Режим доступу или URb: http://corn.com.ua/about.wsp.

ДОДАТОК А

ПЕРЕХРЕСНІ ПОСИЛАННЯ НА СТАНДАРТИ

Таблиця А.1

ISO 9001:2015	ISO 14001:2015	OHSAS 18001:2007	ISO 22000:2005	ISO 27001:2013
Вступ	Вступ	Вступ	Вступ	Вступ
0.1 Загальні положення	0.1 Загальні положення			0.1 Загальні положення
0.2 Принципи управління якістю	0.2 Мета системи управління навколишнім середовищем			
	0.3 Фактори успіху			
0.3 Процесний підхід	0.4 Процесний підхід			
0.4 Зв'язок з іншими стандартами на системи управління				0.2 Зв'язок з іншими стандартами на системи управління
	0.5 Зміст міжнародного стандарту ISO 14001			
1 Сфера застосування	1 Сфера застосування	1 Сфера застосування	1 Сфера застосування	1 Сфера застосування
2 Нормативні посилання	2 Нормативні посилання	2 Нормативні посилання	2 Нормативні посилання	2 Нормативні посилання
3 Терміни і визначення понять	3 Терміни і визначення понять	3. Терміни і визначення понять	3 Терміни і визначення понять	3 Терміни і визначення понять
4 Середовище організації	4 Середовище організації			4 Середовище організації
4.1 Розуміння організації і її середовища	4.1 Розуміння організації і її середовища			4.1 Розуміння організації і її середовища

Продовження таблиці А.1

ISO 9001:2015	ISO 14001:2015	OHSAS 18001:2007	ISO 22000:2005	ISO 27001:2013
4.2 Розуміння потреб і очікувань зацікавлених сторін	4.2 Розуміння потреб і очікувань зацікавлених сторін			4.2 Розуміння потреб і очікувань зацікавлених сторін
4.3 Визначення сфери застосування системи управління якістю	4.3 Визначення сфери застосування системи управління навколишнім середовищем	4 Вимоги до системи управління ГіБП. 4.1 Загальні вимоги	4 Система управління безпечністю харчових продуктів. 4.1 Загальні вимоги	4.3 Визначення сфери застосування системи управління інформаційною безпекою
4.4 Система управління якістю і її процеси	4.4 Система управління навколишнім середовищем	4 Вимоги до системи управління ГіБП. 4.1 Загальні вимоги	4 Система управління безпечністю харчових продуктів. 4.1 Загальні вимоги	4.4 Система управління інформаційною безпекою
5 Лідерство	5 Лідерство		5. Відповідальність керівництва	5 Лідерство
5.1 Лідерство й зобов’язання	5.1 Лідерство і зобов’язання	4.2 Політика у сфері ГіБП. 4.4.1 Ресурси, функціональні обов'язки, відповідальність і повноваження. 4.6 Аналізування з боку керівництва	5.1 Зобов’язання керівництва	5.1 Лідерство й зобов’язання
5.1.1 Загальні положення	5.1.1 Загальні положення	4.2 Політика у сфері ГіБП. 4.4.1 Ресурси, функціональні обов'язки, відповідальність і повноваження. 4.6 Аналізування з боку керівництва		5.1 Лідерство й зобов’язання
5.1.2 Орієнтація на замовника		4.3.1 Ідентифікування небезпек, оцінювання	5.7 Готовність до надзвичайних ситуацій і	

Продовження таблиці А.1

ISO 9001:2015	ISO 14001:2015	OHSAS 18001:2007	ISO 22000:2005	ISO 27001:2013
		ризиків і визначення засобів управління. 4.3.2 Законодавчі та інші вимоги	реагування на них	
5.2 Політика у сфері якості	5.2 Політика у сфері якості	4.2 Політика у сфері ГіБП	5.2 Політика щодо безпечності харчових продуктів	5.2 Політика у сфері якості
5.2.1 Формування політики у сфері якості				5.2.1 Формування політики у сфері якості
5.2.2 Інформування про політику у сфері якості				5.2.2 Інформування про політику у сфері якості
5.3 Функції, обов'язки та повноваження в межах організації	5.3 Функції, обов'язки та повноваження в межах організації	4.1 Загальні вимоги	5.4 Відповідальність і повноваження. 5.5 Керівник групи управління безпечністю харчових продуктів	5.3 Функції, обов'язки та повноваження в межах організації
6 Планування	6 Планування	4.3 Планування		6 Планування
6.1 Дії стосовно ризиків і можливостей	6.1 Дії стосовно ризиків і можливостей	4.3.1 Ідентифікування небезпек, оцінювання ризиків і визначення засобів управління	5.7 Готовність до надзвичайних ситуацій і реагування на них. 7.4 Аналізування небезпечних чинників. 7.4.1 Загальні положення	6.1 Дії стосовно ризиків і можливостей
6.2 Цілі у сфері якості та планування дій для їх досягнення	6.2 Цілі у сфері навколишнього середовища та планування дій для їх досягнення	4.3 Планування. 4.3.3 Цілі й програми	5.3 Планування системи управління безпечністю харчових продуктів	6.2 Цілі у сфері інформаційної безпеки та планування дій для їх досягнення

Продовження таблиці А.1

ISO 9001:2015	ISO 14001:2015	OHSAS 18001:2007	ISO 22000:2005	ISO 27001:2013
6.3 Планування змін			8.5.2 Оновлення системи управління безпечністю харчових продуктів	
7 Підтримання системи управління	7 Підтримання системи управління	4.4.1 Ресурси, функціональні обов'язки, відповідальність і повноваження		7 Підтримання системи управління
7.1 Ресурси	7.1 Ресурси	4.4.1 Ресурси, функціональні обов'язки, відповідальність і повноваження	6 Керування ресурсами	7.1 Ресурси
7.1.1 Загальні положення		4.4.1 Ресурси, функціональні обов'язки, відповідальність і повноваження	6.1 Забезпечення ресурсами	
7.1.2 Людські ресурси		4.4.1 Ресурси, функціональні обов'язки, відповідальність і повноваження	6.2 Людські ресурси. 6.2.1 Загальні положення	
7.1.3 Інфраструктура		4.4.1 Ресурси, функціональні обов'язки, відповідальність і повноваження	6.3. Інфраструктура. 7.2 Програми-передумови (ПП)	
7.1.4 Середовище для функціонування процесів		4.4.1 Ресурси, функціональні обов'язки, відповідальність і повноваження	6.4 Робоче середовище. 7.2.1 Програми-передумови (ПП)	
7.1.5 Ресурси для моніторингу та вимірювання		4.5.1 Вимірювання, результативність і моніторинг	8.3 Керування моніторингом і вимірюваннями	

Продовження таблиці А.1

ISO 9001:2015	ISO 14001:2015	OHSAS 18001:2007	ISO 22000:2005	ISO 27001:2013
7.1.6 Знання організації		4.4.2 Компетентність, підготовленість і обізнаність	6.2.2 Компетентність, підготовленість і обізнаність	
7.2 Компетентність	7.2 Компетентність	4.4.2 Компетентність, підготовленість і обізнаність	6.2.2 Компетентність, підготовленість і обізнаність	7.2 Компетентність
7.3 Обізнаність	7.3 Обізнаність	4.4.2 Компетентність, підготовленість і обізнаність	6.2.2 Компетентність, підготовленість і обізнаність	7.3 Обізнаність
7.4 Інформування	7.4 Інформування	4.4.3 Інформування, участь і консультування	5.6 Інформування	7.4 Інформування
7.5 Задокументована інформація	7.5 Задокументована інформація	4.4.4 Документація	4.2 Вимоги до документації	7.5 Задокументована інформація
7.5.1 Загальні положення	7.5.1 Загальні положення	4.4.4 Документація	4.2.1 Загальні положення	7.5.1 Загальні положення
7.5.2 Створення і актуалізація	7.5.2 Створення і актуалізація	4.4.5 Управління документацією. 4.5.4 Управління записами	4.2.2 Керування документами. 7.7 Оновлення попередньої інформації та документів, які визначають ПП і план НАССР. 4.2.3 Керування протоколами	7.5.2 Створення і актуалізація
7.5.3 Контроль задокументованої інформації	7.5.3 Контроль задокументованої інформації	4.4.5 Управління документацією. 4.5.4 Управління записами	4.2.2 Керування документами. 7.7 Оновлення попередньої інформації та документів, які	7.5.3 Контроль задокументованої інформації

Продовження таблиці А.1

ISO 9001:2015	ISO 14001:2015	OHSAS 18001:2007	ISO 22000:2005	ISO 27001:2013
			визначають ПП і план HACCP 4.2.3 Керування протоколами	
8 Виробництва	8 Функціонування	4.4 Впровадження і функціонування	7 Планування і випуск безпечної продукції	8 Експлуатація
8.1 Оперативне планування й контроль	8.1 Оперативне планування й контроль	4.4.6 Управління операціями	7.1 Загальні положення	8.1 Оперативне планування й контроль
8.2 Вимоги щодо продукції та послуг		4.4.6 Управління операціями	7.3.3 Характеристики продукту	
8.2.1 Інформаційний зв'язок із замовниками				
8.2.2 Визначення вимог щодо продукції та послуг		4.3.1 Ідентифікування небезпек, оцінювання ризиків і визначення засобів управління. 4.3.2 Законодавчі та інші вимоги	7.3.4 Використання за призначеністю	
8.2.3 Аналізування вимог щодо продукції та послуг		4.3.1 Ідентифікування небезпек, оцінювання ризиків і визначення засобів управління		
8.2.4 Зміни до вимог щодо продукції та послуг		4.4.6 Управління операціями	7.6 Установлення плану HACCP	
8.3 Проектування й розробляння продукції та послуг		4.4.6 Управління операціями	7.3 Попередні кроки, щоб уможливити аналіз небезпечних чинників	

Продовження таблиці А.1

ISO 9001:2015	ISO 14001:2015	OHSAS 18001:2007	ISO 22000:2005	ISO 27001:2013
			8.4.2 Оцінювання індивідуальних результатів перевіряння. 8.5.2 Оновлення системи управління безпечністю харчових продуктів	
8.3.1 Загальні положення		4.4.6 Управління операціями	7.3.1 Загальні положення	
8.3.2 Планування проектування й розробляння		4.4.6 Управління операціями	7.3.2 Група управління безпечністю харчових продуктів	
8.3.3 Вхідні дані проектування й розробляння		4.4.6 Управління операціями	7.5 Установлення операційних програм-передумов (ПП)	
8.3.4 Засоби контролю проектування й розробляння		4.4.6 Управління операціями	7.8 Планування перевіряння	
8.3.5 Вихідні дані проектування й розробляння		4.4.6 Управління операціями	7.6 Установлення плану НАССР	
8.3.6 Зміни у проекті й розробці		4.4.6 Управління операціями		
8.4 Контроль надаваних іззовні процесів		4.4.6 Управління операціями	7.3.3 Характеристики продукту	
8.4.1 Загальні положення		4.4 Запровадження і функціонування. 4.4.6 Управління операціями		
8.4.2 Вид та обсяг контролю		4.4.6 Управління операціями	7.2.2 Програми-передумови (ПП).	

Продовження таблиці А.1

ISO 9001:2015	ISO 14001:2015	OHSAS 18001:2007	ISO 22000:2005	ISO 27001:2013
			7.2.3 Програми-передумови (ПП). 7.6.1 План НАССР. 7.6.2 Ідентифікація критичних точок керування (КТК). 7.6.3 Визначення критичних меж для критичних точок керування	
8.4.3 Інформація для зовнішніх постачальників		4.4.6 Управління операціями		
8.5 Виробництво продукції та надання послуг		4.4.6 Управління операціями		
8.5.1 Контроль виготовляння продукції та надання послуг	8.2 Готовність до надзвичайних ситуацій і реагування на них	4.4.6 Управління операціями	7.6.1 План НАССР. 7.6.2 Ідентифікація критичних точок керування (КТК). 7.6.3 Визначення критичних меж для критичних точок	8.2 Оцінювання ризиків щодо інформаційної безпеки. 8.3 Оброблення ризиків щодо інформаційної безпеки
8.5.2 Ідентифікація й простежуваність		4.4.6 Управління операціями	7.9 Система простежуваності	
8.5.3 Власність замовників або зовнішніх постачальників			8.3 Керування моніторингом і вимірюванням	
8.5.4 Збереження		4.4.6 Управління операціями	7.2 Програми-передумови (ПП)	

Продовження таблиці А.1

ISO 9001:2015	ISO 14001:2015	OHSAS 18001:2007	ISO 22000:2005	ISO 27001:2013
8.5.5 Діяльність після постачання		4.4.6 Управління операціями		
8.5.6 Контроль змін		4.4.6 Управління операціями		
8.6 Випуск продукції та послуг		4.4.6 Управління операціями		
8.7 Контроль невідповідних виходів		4.4.7 Готовність до надзвичайних ситуацій і реагування на них	7.6.5 Дії в разі, коли результати моніторингу перевищують критичні межі	
9 Оцінювання дієвості	9 Оцінювання дієвості	4.5 Перевіряння	8 Підтвердження, перевіряння та поліпшування системи управління безпечністю харчових продуктів	9 Оцінювання дієвості
9.1 Моніторинг, вимірювання, аналізування і оцінювання	9.1 Моніторинг, вимірювання, аналізування і оцінювання	4.5.1 Вимірювання, результативність й моніторинг. 4.5.2 Оцінювання дотримання правових вимог	7.6.4 Система моніторингу критичних точок керування. 8.4 Перевіряння системи управління безпечністю харчових продуктів	9.1 Моніторинг, вимірювання, аналізування і оцінювання
9.1.1 Загальні положення	9.1.1 Загальні положення	4.4.7 Готовність до надзвичайних ситуацій і реагування на них	7.6.4 Система моніторингу критичних точок керування	
9.1.2 Задоволеність замовника	9.1.2 Оцінювання виконання забов’язань			
9.1.3 Аналізування та оцінювання		4.5.1 Вимірювання, результативність й моніторинг	8.2 Підтвердження комбінацій заходів керування.	

Продовження таблиці А.1

ISO 9001:2015	ISO 14001:2015	OHSAS 18001:2007	ISO 22000:2005	ISO 27001:2013
			8.4.2 Оцінювання індивідуальних результатів перевіряння. 8.4.3 Аналізування результатів дій щодо перевіряння	
9.2 Внутрішній аудит	9.2 Внутрішній аудит	4.5.5 Внутрішній аудит	8.4.1 Внутрішній аудит	9.2 Внутрішній аудит
9.3 Аналізування системи управління	9.3 Аналізування системи управління	4.6 Аналізування з боку керівництва	5.8 Аналізування з боку керівництва	9.3 Аналізування системи управління
9.3.1 Загальні положення	9.3.1 Загальні положення	4.6 Аналізування з боку керівництва	9.3.1 Загальні положення	9.3.1 Загальні положення
9.3.2 Вхідні дані аналізування системи управління	9.3.2 Вхідні дані аналізування системи управління	4.6 Аналізування з боку керівництва	9.3.2 Вхідні дані аналізування	9.3.2 Вхідні дані аналізування системи управління
9.3.3 Вихідні дані аналізування системи управління	9.3.3 Вихідні дані аналізування системи управління	4.6 Аналізування з боку керівництва	9.3.3 Вихідні дані аналізування	9.3.3 Вихідні дані аналізування системи управління
10 Поліпшування	10 Поліпшування		8.5 Поліпшування	10 Поліпшування
10.1 Загальне положення	10.1 Загальне положення			
10.2 Невідповідність і коригувальні дії	10.2 Невідповідність і коригувальні дії	4.5.3 Розслідування інцидентів, невідповідності, коригувальні й запобіжні дії	7.10 Керування невідповідністю	10.1 Невідповідність і коригувальні дії
10.3 Постійне поліпшування	10.3 Постійне поліпшування	4.2 Політика у сфері ГІБП	8.5.1 Постійне поліпшування	10.2 Постійне поліпшування

ДОДАТОК Б

ПРИКЛАДИ ПОЛІТИК ІНТЕГРОВАНИХ СИСТЕМ УПРАВЛІННЯ

Приклад Б.1

Політика ПрАТ «УКРСТАЛЬКОНСТРУКЦІЯ»

Пріоритетним напрямком діяльності ПрАТ «УКРСТАЛЬКОНСТРУКЦІЯ» [23] (далі - Підприємство) є повне і якісне виконання вимог замовників у наданні професійних послуг з проектування будівель і споруд, виготовлення металоконструкцій, проведення будівельно-монтажних робіт з урахуванням інтересів співробітників Підприємства та інших зацікавлених сторін.

Політика у сфері якості, здоров'я та безпеки праці, охорони навколишнього середовища є вираженням принципів і цінностей роботи Підприємства, основою функціонування і постійного поліпшення інтегрованої системи менеджменту Підприємства відповідно до принципів і вимог міжнародних стандартів ISO 9001:2008, ISO 14001:2004 і OHSAS 18001:2007.

Своє завдання керівництво Підприємства бачить у створенні умов для професійного зростання співробітників, удосконалення професійних навичок, підвищення рівня освіти, стимулювання здорового способу життя, повноцінного відпочинку співробітників.

Для забезпечення захисту довкілля та здоров'я персоналу вище керівництво Підприємства проводить у рамках посадових інструкцій розроблення щорічних і довгострокових програм технічної модернізації виробничих процесів, впровадження технологій, що зменшують шкідливі викиди і сприяють поліпшенню умов праці персоналу.

У своїй роботі ми керуємося такими принципами:

1. Професіоналізм. Основним активом Підприємства є його співробітники, з яких кожен – професіонал у своїй справі або прагне ним стати. Всі співробітники якісно, ефективно виконують поставлені перед ними завдання і постійно прагнуть до вдосконалення своїх навичок, отримання нових знань у своїй професійній діяльності. Тільки команда професіоналів може створювати продукти, якість яких максимально відповідає вимогам замовників.

2. Якість. Ми надаємо продукт і послуги тільки високої якості, які здатні задовольняти встановленим і передбачуваним вимогам замовників. У своїй діяльності співробітники Підприємства прагнуть виконувати свої обов'язки якісно, надавати один одному всіляку допомогу і підтримку з тим, що б рівень якості виробленої продукції відповідав найвищим вимогам Споживача.

Ми висуваємо **високі вимоги** до всіх аспектів нашої діяльності: узгоджена робота партнерів і постачальників, ефективне проходження бізнес-процесів на Підприємстві, взаємовигідне співробітництво з замовником.

3. Удосконалення. У своїй роботі ми постійно прагнемо до розвитку, вдосконалення й втілення нових ідей; розширення знань і компетенції співробітників, активного залучення всього персоналу в поліпшення роботи підприємства, повного розкриття потенційних можливостей співробітників.

4. Конфіденційність. Усі матеріали та інформація, надана замовниками, використовується тільки для досягнення цілей, погоджених із замовниками. Підприємство строго дотримується принципу, що найцінніше у співпраці з нашими замовниками - це довіра.

Керівництво Підприємства бере на себе такі зобов'язання:

– орієнтуватись на виконання вимог споживачів продукції та постійного підвищення їх задоволеності;

– враховувати при виробництві продукції вимоги чинного законодавства, а також інші вимоги, прийняті Підприємством;

– залучати персонал у процес безперервного поліпшення інтегрованої системи менеджменту (ІСМ);

– підтримувати процесну модель управління і безперервно вдосконалювати структуру Підприємства;

– розробляти і реалізовувати програми, спрямовані на зниження негативного впливу діяльності Підприємства на навколишнє середовище, на створення безпечних умов праці;

– постійно покращувати результативність ІСМ у сфері якості, здоров'я та безпеки праці, охорони навколишнього середовища на основі міжнародних стандартів: ISO 9001:2008, ISO 14001:2004 та OHSAS 18001:2007.

Керівництво Підприємства вважає себе відповідальним за створення умов, що дозволяють виконувати і підтримувати всі програми і дії, необхідні для реалізації політики у сфері якості, здоров'я та безпеки праці, охорони навколишнього середовища.

Приклад Б.2

ОАО «Запорожсталь»

ПОЛИТИКА

В ОБЛАСТИ КАЧЕСТВА, ЭНЕРГОЭФФЕКТИВНОСТИ, ОХРАНЫ ТРУДА И ЭКОЛОГИИ

ОАО «Запорожсталь» специализируется на производстве горяче- и холоднокатаного проката из углеродистых, низколегированных, легированных сталей

Являясь ведущим краеобразующим предприятием, комбинат осуществляет свою деятельность, основываясь на принципах устойчивого и социально ответственного бизнеса. Предприятие уделяет особое внимание производству высококачественной продукции, внедрению современных энерго- и ресурсосберегающих технологий, с обязательным учетом природоохранной составляющей, созданию безопасных условий труда — в каждом структурном подразделении и на каждом рабочем месте. Это стремление продиктовано прежде всего осознанием того, что эффективная деятельность предприятия напрямую зависит от его способности функционировать безопасно и с минимальным воздействием на окружающую среду

Руководство предприятия последовательно демонстрирует важность этих ключевых направлений деятельности, устанавливая требования международных стандартов.

Реализация данной Политики предполагает неизменное следование следующим принципам:

— жизнь и здоровье персонала — основная ценность комбината,

— повышение эффективности и непрерывное совершенствование всех бизнес-процессов,

— снижение себестоимости и экономия производства за счет операционной эффективности,

— повышение культуры производства в соответствии с лучшими мировыми практиками.

РУКОВОДСТВО ОАО «ЗАПОРОЖСТАЛЬ» ПРИНИМАЕТ НА СЕБЯ ОБЯЗАТЕЛЬСТВА:

- постоянно совершенствовать и повышать результативность Интегрированной системы менеджмента качества, энергоэффективности, охраны труда, экологии в соответствии с требованиями ISO 9001, ISO 14001, OHSAS 18001, ILO-OSH 2001, ISO 50001;
- соблюдать требования законодательных и нормативно-правовых актов, международных соглашений, отраслевых и корпоративных стандартов, других требований, принятых комбинатом по вопросам качества, энергоэффективности, охраны труда, экологии;
- выпускать качественную, конкурентоспособную металлопродукцию, удовлетворяющую самые высокие требования потребителя;
- использовать элементы программы «Бережливое производство» как инструмента непрерывного совершенствования;
- снижать затраты всех видов ресурсов за счет применения ресурсосберегающих технологий;
- обеспечивать закупку энергоэффективных видов продукции и услуг для улучшения энергетической результативности;
- обеспечивать безопасность производственных процессов и инфраструктуры;
- достигать нулевых показателей производственного травматизма;
- обеспечивать меры по устранению опасностей и снижению рисков, предупреждению травматизма и ухудшения состояния здоровья персонала комбината и работников подрядных организаций;
- уменьшать риск причинения вреда здоровью персонала и негативного воздействия на окружающую среду;
- предотвращать отказы оборудования, инциденты, аварии и экоаспекты;
- обеспечивать все процессы компетентным высококвалифицированным персоналом;
- повышать удовлетворенность персонала за счет создания безопасных условий труда и благоприятной окружающей среды.

Руководство ОАО «Запорожсталь» является гарантом реализации Политики.

Настоящая Политика распространяется на все структурные подразделения ОАО «Запорожсталь», доводится до сведения всех работников комбината, подрядчиков, всех заинтересованных сторон.

Генеральный директор
ОАО «ЗАПОРОЖСТАЛЬ» **Р. И. Шурма**

«___» _____ 2012 г.

Рисунок Б.1 – Політика ВАТ «Запоріжсталь» [25]

Приклад Б.3

Політика «Старснек» в питаннях якості й безпечності продуктів харчування, охорони навколишнього середовища, охорони праці та здоров'я [25]

Ми – підприємство, що виробляє сухі сніданки, а саме:

– кукурудзяні палички солодкі в асортименті;
– кукурудзяні палички молочні;
– фігурні вироби солодкі ароматизовані в асортименті;
– фігурні вироби солоні з різними смаками.

Ми вживаємо заходів для задоволення таких потреб споживачів:

1) якісна і безпечна продукція:

– виробнича діяльність проводиться з дотриманням вимог законодавства, державних стандартів, затверджених технологічних інструкцій, високих внутрішніх вимог до якості і безпечності продукції;

– ми працюємо над постійним удосконаленням технології виробництва, якості сировини та матеріалів;

– постійно відбувається оновлення виробничого обладнання, формування нових та розширення існуючих виробничих ліній;

– періодично організовуються навчання працівників для підвищення кваліфікації та підготовки до впровадження нових стандартів якості;

– проводяться лабораторні дослідження цехів, обладнання, продукції підприємства;

– продукція підприємства не містить генетично модифікованих організмів;

2) широкий вибір сухих сніданків:

– ми постійно розширюємо асортимент продукції, вводячи в нього не лише традиційні кукурудзяні палички, але й інші фігурні вироби з різними смаками, снеки до пива та ін.;

– ми забезпечуємо можливість вибору потрібного розміру тари, що допомагає споживачам контролювати кількість спожитих калорій;

– ми виробляємо продукцію різних цінових категорій, що робить її доступною для широкого кола споживачів;

– придбавши той чи інших продукт, наші споживачі мають змогу взяти участь у різноманітних акціях та розіграшах призів;

3) інформаційна доступність і відкритість підприємства:

– ми відповідально ставимось до надання інформації про свою продукцію, її склад, основні показники: калорійність, енергетичну цінність, вагу, умови зберігання та вживання та ін.;

– підприємство використовує маркування упаковки, що відповідає вимогам законодавства;

– діє інтернет-сторінка підприємства, де відображена інформація про підприємство, про умови акцій, що проводяться, про переможців розіграшів призів, інша корисна для споживача інформація;

4) відповідальність:

– проводиться постійний моніторинг та аналіз, удосконалення системи управління якістю і безпечністю харчової продукції, охорони праці та здоров'я, охорони навколишнього середовища;

– доводяться вимоги до партнерів та постачальників щодо неухильного дотримання стандартів у сфері якості та безпечності продукції;

– забезпечення працівників підприємства матеріально-технічною та інформаційною базою для безпечного і ефективного виконання ними своїх обов'язків.

До наших планів входить таке:

– впровадження та дотримання на підприємстві міжнародних стандартів якості та безпечності харчових продуктів: ISO 9001:2008 (9001:2015), 22000:2005, інших стандартів;

– моніторинг та поступове впровадження нових перспективних технологій виробництва;

– постійне оновлення і розширення асортименту продукції;

– вживання подальших заходів щодо підвищення якості продукції;

– розширення ринку збуту продукції підприємства в Україні, а також вихід на ринки інших країн, зокрема країн Євросоюзу;

– збільшення активності в соціальній сфері.

ДОДАТОК В

ЦІЛІ Й ЗАСОБИ УПРАВЛІННЯ В СУІБ

Цілі й засоби управління щодо забезпечення інформаційної безпеки наведено в таблиці В.1. Перелік, поданий в таблиці не є вичерпним, в організації можна визначити додаткові цілі й засоби управління, які необхідні їй для ефективної інформаційної безпеки. Цілі управління і засоби управління з таблиці В.1 мають бути вибрані як частина процесу СУІБ, визначеного в пп. 3.4.2.1.

Таблиця В.1

Розділ	Елемент СУІБ	Засоби управління
В.3.5	**Політика інформаційної безпеки**	
В.3.5.1 Мета	**Політика керівництва щодо інформаційної безпеки** Забезпечити спрямованість і підтримку з боку керівництва для захисту інформації відповідно до ділових вимог, а також законів і норм, що стосуються справи	
В.3.5.1.1	Документальне оформлення політики у сфері інформаційної безпеки	Документ політики у сфері інформаційної безпеки має бути затверджений керівництвом, а також опублікований і доведений до відома всіх співробітників і стосуватися справи зацікавлених сторін
В.3.5.1.2	Аналізування політики у сфері інформаційної безпеки	Політику у сфері інформаційної безпеки необхідно аналізувати через заплановані інтервали часу або у разі виникнення значних змін з метою гарантування її безперервної придатності, адекватності і результативності
В.3.6	**Організація інформаційної безпеки**	
В.3.6.1 Мета	**Внутрішня організація** Розробити структуру управління з метою ініціювання і управління впровадженням і забезпеченням інформаційної безпеки в рамках організації	
В.3.6.1.1	Ролі та відповідальність за інформаційну безпеку	Вся відповідальність за інформаційну безпеку має бути чітко визначена та закріплена за відповідними особами
В.3.6.1.2	Розподіл відповідальності	Зобов'язання і відповідальність, які викликають протиріччя, слід розподіляти з метою зниження можливості виникнення несанкціонованого випадкового внесення змін або невідповідного використання активів організації
В.3.6.1.3	Контакти з владою	Слід підтримувати належні контакти з компетентними органами
В.3.6.1.4	Контакти зі спеціальними групами фахівців	Необхідно підтримувати належні контакти зі спеціальними групами або іншими форумами фахівців щодо захисту інформації, а також професійними асоціаціями

Продовження таблиці В.1

Розділ	Елемент СУІБ	Засоби управління
В.3.6.1.5	Інформаційна безпека при управлінні проектами	Необхідно забезпечувати інформаційну безпеку при управлінні проектами незалежно від типу проекту
В.3.6.1.5	Угоди конфіденційності	Вимоги до конфіденційності або угоди про нерозголошення, що відображають потреби організації у захисті інформації, мають бути визначенимм і регулярно аналізуватися
В.3.6.2 Мета	**Мобільні пристрої й дистанційна робота** Забезпечити безпечність віддаленої роботи і використання мобільних пристроїв	
В.3.6.2.1	Політика щодо мобільних пристроїв	Мають бути прийняті політика й відповідні дії щодо забезпечення безпеки інформації з метою управління ризиками, які пов'язані з застосуванням мобільних пристроїв
В.3.6.2.2	Дистанційна робота	Мають бути прийняті політика і відповідні дії щодо забезпечення безпеки інформації, захисту доступу до інформації, її оброблення або зберігання при дистанційній роботі
В.3.7	**Безпека інформації, яка пов'язана з людськими ресурсами**	
В.3.7.1 Мета	**Перед прийняттям на роботу** Гарантувати, що службовці й підрядники розуміють свою відповідальність і можуть посідати місця, на які їх пропонують	
В.3.7.1.1	Перевірка благонадійності	Необхідно перевіряти інформацію стосовно всіх кандидатів на посади в організації згідно з відповідними законами, нормами, етикою, професійними вимогами, класифікацією інформації, до якої матиме доступ особа, та можливими ризиками
В.3.7.1.2	Умови працевлаштування	В умовах договору особистого найму співробітників і підрядників необхідно вказати їх відповідальність за захист інформації
В.3.7.2 Мета	**Під час роботи** Гарантувати, що всі службовці та підрядники усвідомлюють свої відповідальність і зобов'язання в рамках забезпечення інформаційної безпеки	
В.3.7.2.1	Відповідальність керівництва	Керівництво має вимагати від службовців, підрядників і користувачів третьої сторони захищати інформацію відповідно до встановленої політики і процедур організації
В.3.7.2.2	Поінформованість, освіта і підготовка у сфері інформаційної безпеки, навчання й інструктажі	Усі службовці організації і, якщо це стосується справи, підрядники і користувачі третьої сторони, мають отримати відповідну підготовку з підвищення кваліфікації та регулярні оновлення організаційної політики і процедур, наскільки це належить до їхніх робочих функцій
В.3.7.2.3	Дисциплінарний процес	Має бути розроблено процес дисциплінарного стягнення для співробітників, дії яких призвели до порушення захисту інформації

Продовження таблиці В.1

Розділ	Елемент СУІБ	Засоби управління
В.3.7.3 Мета	**Звільнення або зміненння посади** Захищати інтереси організації при звільненні або зміненні посади співробітника	
В.3.7.3.1	Звільнення або змінення професійних обов'язків	Мають бути визначені, доведені до співробітника чи підрядника відповідальність і повноваження щодо інформаційної безпеки, які залишаються у співробітника після його звільнення або змінення його професійних зобов'язань
В.3.8	**Управління активами**	
В.3.8.1 Мета	**Відповідальність за активи** Необхідно визначити активи організації та відповідальність щодо їхнього захисту	
В.3.8.1.1	Інвентаризація активів	Мають бути визначені активи організації, які пов'язані з інформацією і засобами її оброблення, а також складено реєстр цих активів, який необхідно постійно переглядати
В.3.8.1.2	Власники активів	Мають бути визначені власники активів, які занесено до реєстру
В.3.8.1.3	Допустиме використання активів	Слід визначити, задокументувати та впровадити правила допустимого використання інформації й активів, які пов’язані з нею і засобами її оброблення
В.3.8.1.4	Повернення активів	Усі службовці, підрядники і користувачі третьої сторони мають повернути організації всі активи, що знаходяться в їхньому володінні, коли закінчиться термін дії трудового договору або угоди
В.3.8.2 Мета	**Класифікація інформації** Гарантувати, що різні види інформації будуть належним чином захищені відповідно до їхнього значення для функціонування організації	
В.3.8.2.1	Настанова щодо класифікації	Інформація має бути класифікована з погляду її значення, законодавчих вимог, уразливості й критичності для організації
В.3.8.2.2	Маркування і оброблення інформації	Відповідно до схеми класифікації, прийнятої в організації, має бути розроблено і реалізовано встановлений набір процедур маркування і оброблення інформації
В.3.8.2.3	Відповідне застосування активів	Процедури відповідного застосування активів мають бути розроблені й впроваджені згідно з прийнятою в організації схемою класифікації інформації
В.3.8.3 Мета	**Відповідне застосування носіїв інформації** Запобігати недозволеному розголошенню, зміні, видаленню або знищенню інформації, яка зберігається на носіях інформації	

Продовження таблиці В.1

Розділ	Елемент СУІБ	Засоби управління
В.3.8.3.1	Контролювання знімних носіїв інформації	Мають бути вжиті процедури контролювання знімних носіїв інформації згідно з прийнятою в організації схемою класифікації інформації
В.3.8.3.2	Ліквідація носіїв інформації	Якщо носій більше не потрібен, то він має бути надійно і безпечно ліквідований згідно з формальною процедурою
В.3.8.3.3	Фізичне транспортування носіїв інформації	Носії інформації мають бути захищені від несанкціонованого доступу, невідповідного використання або пошкодження під час їхнього транспортування
В.3.9	**Управління доступом**	
В.3.9.1 Мета	**Вимоги бізнесу до управління доступом** Запобігти недозволеному доступу до інформації і засобам її оброблення	
В.3.9.1.1	Політика управління доступом	Політика управління доступом має бути розроблена, задокументована й аналізуватися згідно з вимогами бізнесу і системи управління інформаційною безпекою організації
В.3.9.1.2	Доступ до мереж і мережних послуг	Доступ до мереж і мережних послуг користувачам слід надавати тільки в тих випадках, коли вони мають офіційні повноваження для цього
В.3.9.2 *Мета*	**Контролювання доступу користувачів** Гарантувати доступ зареєстрованим користувачам і запобігати недозволеному доступу до інформаційних систем	
В.3.9..2.1	Реєстрація і відміна реєстрації користувачів	Мають бути встановлені формальні процедури реєстрації і зняття з реєстрації користувачів з метою надання і анулювання доступу до всіх інформаційних систем і послуг
В.3.9.2.2	Ініціалізування доступу користувачів	Має бути впроваджено формальний процес ініціалізування доступу для встановлення і анулювання прав доступу до всіх інформаційних систем і послуг
В.3.9.2.3	Контролювання привілеїв	Призначення і використання привілеїв має бути обмежене і контрольоване
В.3.9.2.4	Контролювання аутентифікації користувачів конфіденційною інформацією	Аутенфікацію користувачів конфіденційною інформацією слід контролювати через формалізований процес управління
В.3.9.2.5	Перегляд прав користувачів	Власники активів мають регулярно переглядати права доступу користувачів до активів
В.3.9.2.6	Відміна або зміна прав доступу користувачів до інформації	Права доступу до інформації та засобам її оброблення всіх співробітників і представників сторонніх організацій необхідно відміняти або змінювати, коли закінчиться термін дії трудового договору або угоди

Продовження таблиці В.1

Розділ	Елемент СУІБ	Засоби управління
В.3.9.3 Мета	**Відповідальність користувачів** Забезпечити виконання користувачами процедури аутентифікації	
В.3.9.3.1	Користування конфіденційною інформацією	Користувачі мають виконувати вимоги організації щодо використання конфіденційної інформації
В.3.9.4 Мета	**Управління доступом до мережі і додатків** Запобігати недозволеному доступу до систем і додатків	
В.3.9.4.1	Обмеження доступу до інформації	Доступ до інформації і функціям прикладних систем має бути обмеженим згідно з політикою управління доступом
В.3.9.4.2	Процедури захищеного входу у систему	За необхідності доступ до систем і додатків слід забезпечувати за допомогою процедури захищеного входу згідно з політикою управління доступом
В.3.9.4.3	Система контролювання паролів	Система контролювання паролів має бути інтерактивною і забезпечувати якість паролей
В.3.9.4.4	Застосування системних утиліт	Необхідно обмежити і контролювати використання утиліт, які можуть управляти системою і додатками
В.3.9.4.5	Контроль доступу до початкових кодів програм	Доступ до початкових кодів програм має бути обмежено
В.3.10	**Криптографія**	
В.3.10.1 Мета	**Контроль засобів криптографії** Забезпечити коректне і ефективне застосування засобів криптографії для захисту конфіденційності, достовірності і / або цілісності інформації	
В.3.10.1.1	Політика застосування засобів криптографії	Політика застосування засобів криптографії для захисту інформації має бути розроблена і впроваджена в організації
В.3.10.1.2	Контроль ключів	Політика щодо застосування і захисту криптографічних ключів має бути розроблена і впроваджена в рамках усього життевого циклу системи
В.3.11	**Фізичний захист і захист від навколишнього середовища**	
В.3.11.1 Мета	**Зони безпеки** Запобігти недозволеному фізичному доступу, збиткам і втручанню в нерухомість і інформацію організації	
В.3.11.1.1	Фізична зона безпеки	Для захисту зон, в яких знаходяться інформація і засоби оброблення інформації, слід використовувати заходи безпеки (бар'єри, такі як стіни, керований картами турнікет на вході або контрольовану людиною вахту)
В.3.11.1.2	Управління фізичним доступом	Зони безпеки мають бути захищені відповідними засобами управління для забезпечення того, щоб доступ було дозволено тільки вповноваженому персоналу

Продовження таблиці В.1

Розділ	Елемент СУІБ	Засоби управління
В.3.11.1.3	Організація захисту офісів, приміщень і обладнання	Має бути розроблено і застосовано фізичний захист офісів, приміщень і обладнання
В.3.11.1.4	Захист проти зовнішніх і екологічних загроз	Має бути розроблено і застосовано фізичний захист проти збитків, спричинених вогнем, повінню, землетрусом, вибухом, громадськими безладами та іншими формами природного або штучного лиха
В.3.11.1.5	Робота в небезпечних зонах	Має бути розроблено і застосовано фізичний захист і відповідні процедури для роботи в небезпечних зонах
В.3.11.1.6	Зони загального доступу постачання і завантаження	Місця доступу, такі як зони постачання і завантаження, а також інші місця, куди, не маючи дозволу, не можуть увійти будь-які особи, слід охороняти і, якщо можливо, ізолювати від засобів оброблення інформації з метою уникнути недозволеного доступу до них
В.3.11.2 Мета	**Захист обладнання** Запобігти небезпеці, збитку, крадіжці або компрометації активів і заміні обладнання в роботі організації	
В.3.11.2.1	Розміщення і захист обладнання	Обладнання має бути розміщене і захищене так, щоб знизити ризики від загроз і небезпек навколишнього середовища, а також від можливого недозволеного доступу людей
В.3.11.2.2	Допоміжне обладнання	Обладнання має бути захищене від порушень енергопостачання та інших порушень в роботі допоміжного обладнання
В.3.11.2.3	Захист кабельної системи	Джерело енергії й кабелі зв'язку, за допомогою яких передають дані або допоміжні інформаційні послуги, мають бути захищені від перехоплення або пошкодження
В.3.11.2.4	Технічне обслуговування обладнання	Обладнання слід обслуговувати відповідним чином, щоб гарантувати постійну його доступність і цілісність
В.3.11.2.5	Переміщення активів	Обладнання, інформацію або програмне забезпечення не слід виносити за межі зони безпеки без попереднього дозволу
В.3.11.2.6	Захист обладнання і активів поза територією організації	Має бути забезпечено захист обладнання і активів з урахуванням різних ризиків, які пов’язані з роботою за межами приміщень і території організації
В.3.11.2.7	Безпечна ліквідація або повторне використання обладнання	Усі одиниці обладнання, що містять носії інформації, слід перевіряти, щоб гарантувати, що будь-які вразливі дані і ліцензоване програмне забезпечення було видалено або надійно перезаписано перед ліквідацією

Продовження таблиці В.1

Розділ	Елемент СУІБ	Засоби управління
В.3.11.2.8	Обладнання користувача, яке працює в автоматичному режимі	Користувачі мають гарантувати, що обладнання, яке працює в автоматичному режимі, має відповідний захист
В.3.11.2.9	Політика чистого столу і чистого екрану	Має бути прийнята політика чистого столу для паперів і знімних носіїв і політика чистого екрану для засобів, що обробляють інформацію
В.3.12	**Контроль засобів зв'язку і експлуатації**	
В.3.12.1 Мета	**Процедури експлуатації й відповідальності** Гарантувати відповідну і безпечну роботу засобів оброблення інформації	
В.3.12.1.1	Документовані процедури експлуатації	Процедури експлуатації мають бути документованими, підтримуватися в робочому стані і доступними для всіх користувачів, яким вони потрібні
В.3.12.1.2	Контроль змін	Зміни в організації, бізнес-процесах, засобах і системах оброблення інформації слід контролювати
В.3.12.1.2	Контроль потужностей	Застосування ресурсів слід контролювати згідно з актуальними потребами і прогнозами на майбутнє стосовно необхідної продуктивності системи
В.3.12.1.3	Розподіл засобів розроблення, тестування і експлуатації	Засоби розроблення, випробування і експлуатації слід розділити з метою знизити ризики недозволеного доступу до систем експлуатації або змін в них
В.3.12.2 Мета	**Захист від шкідливого програмного забезпечення** Захистити цілісність програмного забезпечення (ПЗ) й інформації	
В.3.12.2.1	Засоби захисту від шкідливого ПЗ	Мають бути реалізовані засоби управління, виявлення, запобігання і відновлення з метою захисту інформації від шкідливого ПЗ, а також здійснені належні процедури підвищення обізнаності користувачів
В.3.12.3 Мета	**Резервне копіювання** Підтримувати цілісність і доступність інформації та засобів оброблення інформації	
В.3.12.3.1	Резервне копіювання інформації	Резервні копії інформації і програмного забезпечення слід регулярно знімати і перевіряти відповідно до погодженої політики резервного копіювання
В.3.12.4 Мета	**Логи і моніторинг** Запис подій та отримання фактичних даних	
В.3.12.4.1	Ведення журналу подій (логів)	Журнали подій, в які записують дії користувачів, винятки і події в роботі системи захисту інформації, слід вести, зберігати протягом визначеного періоду часу і постійно аналізувати

Продовження таблиці В.1

Розділ	Елемент СУІБ	Засоби управління
В.3.12.4.2	Захист інформації в логах	Засоби ведення логів й інформація в них мають бути захищені від фальсифікації і недозволеного доступу
В.3.12.4.3	Логи адміністратора і оператора	Дії системного адміністратора і оператора необхідно реєструвати, логи мають бути захищені та постійно аналізуватися
В.3.12.4.4	Синхронізація годинників	Годинники всіх причетних до справи систем оброблення інформації в межах організації або зони безпеки мають бути синхронізовані з визнаним джерелом точного часу
В.3.12.5 Мета	**Контроль системного програмного забезпечення** Забезпечити цілісність операційних систем (ОС)	
В.3.12.5.1	Установлення ПЗ на ОС	В організації мають бути впроваджені процедури контролю встановлення ПЗ на ОС
В.3.12.6 Мета	**Контроль технічних вразливостей** Попереджування застосування технічних вразливостей	
В.3.12.6.1	Контроль технічних вразливостей	Інформація про технічні вразливості інформаційних систем, які застосовуються в організації, має надходити своєчасно. Незахищеність організації від таких вразливостей слід оцінювати і приймати відповідні дії для зниження пов’язаного з цим ризику
В.3.12.6.2	Обмеження на встановлення ПЗ	В організації мають бути розроблені й впроваджені правила, які регулюють встановлення ПЗ користувачам
В.3.12.7 Мета	**Проведення аудиту інформаційних систем** Мінімізувати вплив аудиторської діяльності на діючі в організації системи	
В.3.12.7.1	Аудит інформаційних систем	Вимоги до аудиту і діяльність, яка є частиною процесу перевіряння діючих в організації систем, мають бути ретельно сплановані й узгоджені, щоб мінімізувати вірогідність виникнення порушень в бізнес-процесах
В.3.13	**Безпечність зв’язку**	
В.3.13.1 Мета	**Управління мережною безпекою** Забезпечити захист інформації в мережах і засобах оброблення інформації, які підпримують зв'язок з мережею	
В.3.13.1.1	Мережні елементи управління	Для захисту інформації в системах і додатках слід управляти і контролювати мережі
В.3.13.1.2	Безпечність мережних сервісів	Механізми безпечності, рівень сервісів і вимоги до управління всіма мережними сервісами мають бути визначено та внесено до згоди на мережні сервіси як в самій організації, так і для аутсорсингу
В.3.13.1.3	Розподіл в мережах	Групи інформаційних служб і користувачів, інформаційні системи мають бути розділені в мережах

Продовження таблиці В.1

Розділ	Елемент СУІБ	Засоби управління
В.3.13.2 Мета	**Обмін інформацією** Підтримувати інформаційну безпеку і програмне забезпечення в організації і якому-небудь зовнішньому об'єкті	
В.3.13.1.1	Політика і процедури обміну інформацією	Мають бути застосовані офіційна політика і процедури обміну, засоби управління обміном, щоб захистити обмін інформацією через використання всіх типів засобів зв'язку
В.3.13.2.2	Угоди з обміну інформацією	Між організацією і зовнішніми сторонами мають бути встановлені угоди для обміну інформацією та програмним забезпеченням
В.3.13.2.3	Електронний обмін повідомленнями	Інформація, яка включена в електронний обмін повідомленнями, має бути захищена належним чином
В.3.13.2.4	Угоди про нерозголошення інформації (NDA)	Має бути встановлено вимоги до угод про нерозголошення інформації, які відображають потреби організації до захисту інформації. Вимоги до NDA необхідно регулярно аналізувати і документувати
В.3.14	**Придбання, розроблення і підтримування в робочому стані інформаційних систем**	
В.3.14.1 Мета	**Вимоги до захисту інформаційних систем** Гарантувати, що захист є невід'ємною частиною інформаційних систем	
В.3.14.1.1	Аналізування і специфікація вимог до захисту інформації	У формулюваннях ділових вимог до нових інформаційних систем або поліпшень існуючих інформаційних систем мають бути визначені вимоги до засобів управління захистом
В.3.14.1.2	Безпечність прикладних сервісів у загальнодоступних мережах	Інформація, яка внесена до прикладних сервісів і проходить через загальнодоступні мережі, має бути захищена від шахрайської діяльності, несанкціанованого розкриття і модифікації
В.3.14.1.3	Захист транзакцій прикладних сервісів	Інформація, яка внесена в транзакцію прикладних сервісів, має бути захищена задля попередження її передачі не в повному обсязі, а також від невірної маршрутизації, несанкціонованого змінення повідомлення, розкриття, дублювання або відображення повідомлення
В.3.14.2 Мета	**Захист при розробленні і допоміжних процесах** Підтримувати захист прикладного системного програмного забезпечення та інформації	
В.3.14.2.1	Політика безпеки при розроблянні	В організації мають бути встановлені та застосовані правила щодо розроблення ПЗ і систем
В.3.14.2.2	Процедури управління змінами в системі	Реалізацію змін в рамках життєвого циклу розроблянння слід контролювати шляхом використання формальних процедур управління змінами

Продовження таблиці В.1

Розділ	Елемент СУІБ	Засоби управління
В.3.14.2.3	Технічний аналіз додатків після внесення змін до операційної системи	Коли операційні системи змінюються, ділові критичні додатки необхідно аналізувати і тестувати, щоб гарантувати відсутність несприятливого впливу на організаційні операції або їх захист
В.3.14.2.4	Обмеження можливості внесення змін в пакети програм	Змінами в пакетах програм не слід заохочуватися, має бути введено обмеження можливості внесення змін, і всіма змінами необхідно строго управляти
В.3.14.2.5	Принципи безпечності інженерних систем	В організації слід розробляти, документувати, підтримувати і застосовувати до будь-яких інформаційних систем при їхньому впровадженні принципи безпечності інженерних систем
В.3.14.2.6	Безпечне середовище розробляння системи	В організації слід встановити і відповідно захищати безпечне середовище розробляння та інтегрування, яке охоплює весь життєвий цикл системи
В.3.14.2.7	Аутсорсингове розробляння системи	Розробляння системи аутсорсинговою компанією має бути під наглядом і постійним контролем організації
В.3.14.2.8	Тестування захисту системи	Тестування функціональних можливостей захисту системи необхідно проводити в процесі її розроблення
В.3.14.2.9	Прийняття результатів тестування системи	Прийняття результатів тестування програм і критеріїв має бути застосовано для нових інформаційних систем, а також для оновлень і нових версій уже впроваджених в організації систем
В.3.14.3 Мета	**Дані, які тестуються** Забезпечити захист даних, які використовуються під час тестування	
В.3.14.3.1	Захист даних, які тестуються	Дані, які використовуються під час тестування, мають бути ретельно підібрані, захищені й постійно контрольовані
В.3.15	**Взаємовідносини з постачальниками**	
В.3.15.1 Мета	**Інформаційна безпека при взаємовідносинах з постачальниками** Забезпечити захист активів організації, до яких мають доступ постачальники	
В.3.15.1.1	Політика інформаційної безпеки при взаємовідносинах з постачальниками	Для зменшення ризиків, які пов’язані з доступом постачальників до активів організації, слід узгодити і задокументувати вимоги до інформаційної безпеки
В.3.15.1.2	Внесення вимог до інформаційної безпеки активів в договір з постачальником	Всі відповідні вимоги до інформаційної безпеки мають бути встановлені й погоджені з кожним постачальником, який може отримати доступ до інформації організації (її оброблення, зберігання, процесу взаємодії) або бути компонентом ІТ-інфраструктури

Продовження таблиці В.1

Розділ	Елемент СУІБ	Засоби управління
В.3.15.1.3	Інформаційно-комунікаційні технології ланцюга постачань	Угоди з постачальниками мають містити вимоги до зниження ризиків інформаційної безпеки, які пов'язані з інформаційно-комунікаційними технологіями і ланцюгом постачань продукції
В.3.15.2 Мета	**Управління постачаннями** Підтримувати узгоджений рівень інформаційної безпеки і надання послуг відповідно до угод з постачальниками	
В.3.15.2.1	Моніторинг й аналізування послуг, які надає постачальник	В організації слід регулярно проводити моніторинг, аналіз і аудит послуг, які надає постачальник
В.3.15.2.2	Управління змінами послуг, які надає постачальник	Змінами в послугах, які надає постачальник, враховуючи підтримку інформаційної безпеки, процедур і елементів управління, слід управляти з врахуванням критичності бізнес-інформації, систем і процесів, а також повторного оцінювання ризиків
В.3.16	**Управління інцидентами в системі захисту інформації**	
В.3.16.1 Мета	Гарантувати застосування послідовного і результативного підходу до контролю інцидентів у системі захисту інформації	
В.3.16.1.1	Відповідальність і процедури	Мають бути встановлені відповідальність керівництва і процедури для забезпечення швидкої, результативної і впорядкованої реакції на інциденти в системі захисту інформації
В.3.16.1.2	Повідомлення про події в системі захисту інформації	Інформацію про події, які відбуваються в системі захисту інформації, слід повідомляти через відповідні службові канали в найкоротші терміни
В.3.16.1.3	Повідомлення про слабкі місця в системі захисту інформації	Усіх службовців, підрядників і сторонніх користувачів інформаційних систем і послуг необхідно сповіщати через систему інформування про систематичні або підозрілі слабкі місця в системах або послугах
В.3.16.1.4	Оцінюваннння подій щодо інформаційної безпеки й приняття рішень	Події щодо інформаційної безпеки слід оцінювати і, якщо їх класифіковано як інциденти, то відносно них мають прийматися відповідні рішення
В.3.16.1.5	Реагування на інциденти в інформаційній безпеці	Методи реагування на інциденти в інформаційній безпеці мають бути визначені згідно з задокументованими процедурами, які застосовуються в організації
В.3.16.1.6	Отримання досвіду внаслідок виникнення інцидентів в системі захисту інформації	Слід застосовувати механізми для того, щоб дати можливість визначати кількість типів інцидентів, їх обсяги і витрати на усунення їх наслідків в системі захисту інформації і постійно контролювати такі інциденти

Продовження таблиці В.1

Розділ	Елемент СУІБ	Засоби управління
В.3.16.1.7	Збір свідоцтв	Якщо після інциденту, що виник в системі захисту інформації, проти особи або організації подано судовий позов (цивільний або кримінальний), то необхідно зібрати, зберегти і надати свідоцтва з метою підтвердження відповідності правилам стосовно свідчень, установленим у визначеній юрисдикції (юрисдикціях)
В.3.17	**Аспекти інформаційної безпеки управління безперервністю бізнесу**	
В.3.17.1 Мета	**Безперервність інформаційної безпеки** Безперервність інформаційної безпеки має бути невід'ємною частиною системи управління безперервністю бізнесу організації	
В.3.17.1.1	Планування безперервності інформаційної безпеки	В організації мають бути визначені свої вимоги до інформаційної безпеки і її безперервного функціонування, якщо виникає несприятлива ситуація, наприклад, криза або стихійне лихо
В.3.17.1.2	Впровадження процесу безперервності інформаційної безпеки	Необхідно розробляти і підтримувати в робочому стані керований процес для забезпечення безперервності бізнесу всієї організації, щоб задовольнити вимоги захисту інформації
В.3.17.1.3	Тестування, постійний контроль і оцінювання процесу безперервності інформаційної безпеки	В організації необхідно регулярно тестувати і оновлювати процес безперервності інформаційної безпеки з метою гарантувати, що він поповнюється сучасними даними і є результативним щодо забезпечення безперервності бізнесу
В.3.17.2 Мета	**Надмірність** Забезпечити доступність засобів оброблення інформації	
В.3.17.2.1	Доступність засобів оброблення інформації	Кількість засобів оброблення інформації має бути надмірною, щоб задовольнити вимоги стосовно їхньої доступності
В.3.18	**Відповідність вимогам**	
В.3.18.1 Мета	**Відповідність законодавчим і договірним вимогам** Уникати порушень будь-яких законодавчих, статутних, нормативних і договірних зобов'язань і будь-яких вимог захисту	
В.3.18.1.1	Визначення застосовних законодавчих і договірних вимог	Вимоги закону, нормативні і договірні вимоги, а також способи виконання цих вимог в організації мають бути чітко визначеними, документованими і поповнюватися останніми даними для кожної інформаційної системи організації
В.3.18.1.2	Права на інтелектуальну власність (IPR)	Мають бути реалізовані необхідні процедури, щоб гарантувати відповідність законодавчим, нормативним і договірним вимогам використання матеріалу, в якому можуть міститися права на інтелектуальну власність, і ліцензійних програмних продуктів

ЗМІСТ

Навчальне видання

Сіроклин Віталій Павлович
Чернобай Ніна Валеріївна
Бондаренко Ганна Геннадіївна
Глебова Марина Володимирівна
Косач Наталія Ігорівна

ІНТЕГРОВАНІ СИСТЕМИ УПРАВЛІННЯ ЯКІСТЮ

Редактор В. М. Коваль

Зв. план, 2016
Підписано до друку 01.09.2016
Формат 60×84 1/16. Папір офс. № 2. Офс. друк.
Ум. друк. арк. 5,1. Обл.-вид. арк. 5,75. Наклад 100 пр. Замовлення 254.
Ціна вільна

Видавець і виготовлювач
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»
61070, Харків–70, вул. Чкалова, 17
http://www.khai.edu
Видавничий центр «ХАІ»
61070, Харків–70, вул. Чкалова, 17
izdat@khai.edu

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції сер. ДК № 391 від 30.03.2001