

БЕКІТЕМІН

Жәңгір хан атындағы Батыс
Қазақстан аграрлық-техникалық
университеті ҚеАТ

басқарма төрағасы – ректор

" 10 " _____ 2023 ж.



ЦИФРЛЫҚ ДАМУ ОРТАЛЫҒЫНЫҢ АҚПАРАТТЫ ҚОРҒАУ ЖӨНІНДЕГІ БАС МАМАНЫНЫҢ

ЛАУАЗЫМДЫҚ НҰСҚАУЛЫҒЫ

СМЖ.07.ЛН. 196

№ 00 басылым

№ _____ дана

Дайындалды: 04.05.2023 м. Камалова Г. А.	Келісілді: 05.05.2023 м. Таубаев У. Б. Алмагамбетова М. Ж. Ихсанов Е. Б. Таскалиев Е.К.	Енгізілді: 11.05.2023 м. Алғашқы рет Қайта қаралуы: 11.05.2026 м.
---	---	--

Мазмұны

1. Бағыты
2. Қолдану саласы
3. Лауазымдық міндеттері
4. Жауапкершілігі мен құқығы
5. Сілтемелер

Өзгерістер				
№	Енгізілген мерзімі	Беттер нөмірі	Дайындаушы	
			Тегі, аты, әкесінің аты	Қолы

1. Бағыты

Бұл нұсқаулық Қазақстан Республикасының Еңбек кодексіне, «Білім туралы» Заңына сәйкес дайындалды.

2. Қолдану саласы

Бұл нұсқаулық Цифрлық даму орталығының ақпаратты қорғау жөніндегі бас маманына арналған.

3. Лауазымдық міндеттері

3.1. Ақпаратты қорғау жөніндегі бас маман міндетті:

3.1.1. Ұйымның бірінші басшысының және оның орынбасарларының жалпы басшылығымен және өзге бөлімшелер мен қызметтердің басшыларымен өзара әрекеттестікте өз міндеттерін орындайды;

3.1.2. Өз құзыреті шегінде тиісті құрылымдық бөлімшелердің (қызметтердің) қызметіне бөлімшенің жұмысын бағыттау және үйлестіру бойынша басшылық жасайды, әкімшілік мәселелерді шешеді;

3.1.3. Құпия мәліметтерді қорғау және құпиялық режимін қамтамасыз ету мақсатында қолда бар барлық ұйымдастырушылық және техникалық шараларды тиімді қолдануды қамтамасыз ете отырып, экономикалық қызмет түрінде, ұйымда ақпаратты кешенді қорғау бойынша жұмыстарды орындауға басшылық жасайды;

3.1.4. Техникалық бақылау құралдарының техникалық саясатын әзірлеуге және даму перспективаларын айқындауға қатысады, құпия ақпаратқа енуге жол бермейтін немесе біршама қиындататын техникалық және бағдарламалық-математикалық қорғаныш құралдарын әзірлеуді және енгізуді ұйымдастырады;

3.1.5. Бұйымдардың жобаларына арналған техникалық тапсырмаларды, қорғалуға тиіс ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстарды қарауға қатысады, оларға ақпаратты қорғау жөніндегі нормативтік-техникалық және әдістемелік құжаттардың талаптарын енгізуді және осы талаптардың орындалуын бақылауды жүзеге асырады;

3.1.6. Ақпарат жүйелерін қорғау жөніндегі ұйымдастырушылық және инженерлік-техникалық шараларды жұмыс жоспарларымен бағдарламаларына енгізу үшін ұсыныстар дайындайды;

3.1.7. Ақпаратты кешенді қорғау талаптарына сәйкес келетін қауіпсіз ақпараттық технологияларды құру бойынша жұмыстарға қатысады;

3.1.8. Ақпаратты қорғау жүйесін жетілдіру және олардың тиімділігін арттыру саласындағы ғылыми-зерттеу жұмыстарын жүргізуді ұйымдастырады;

3.1.9. Әзірленген бағдарламалар мен әдістемелер негізінде ақпаратты бақылауға және қорғауға байланысты жұмыстардың (оның ішінде ерекше күрделі) барлық кешенін орындайды;

3.1.10. Ақпаратты қорғауды қамтамасыз ету бойынша жұмыстарды жүргізу үшін қажетті арнайы бұйымдарды (өнімдерді) құруға және өндіруге байланысты зерттеулер мен әзірлемелерді жүргізу кезінде ақпараттың жария болып қалу, оның ішінде техникалық арналар бойынша ықтималдығы туралы материалдарды жинауды және талдауды ұйымдастырады;

3.1.11. Жүргізілетін ұйымдастырушылық-техникалық іс-шараларды үйлестіруді, әдістемелік және нормативтік материалдарды әзірлеуді және ақпаратты қорғау, ұсынылатын және іске асырылап жатқан ұйымдастырушылық-техникалық шешімдерді техникалық-экономикалық тиімділігін бағалау жөніндегі жұмысты жүргізуде қажетті әдістемелік көмек көрсетуді қамтамасыз етеді;

3.1.12. Қорғалуға жататын объектілер және қорғалатын мәліметтер туралы қажетті ақпаратты жинау және жүйелеу бойынша жұмысты ұйымдастырады, ақпаратты қорғау жөнінде әзірленген шаралардың техникалық-экономикалық деңгейін және тиімділігін бағалау бойынша жұмысқа әдістемелік басшылық және бақылау жасауды жүзеге асырады.

3.1.13. Ақпарат қорғаудың техникалық және бағдарламалық-математикалық құралдарына, бақылау аппаратурасына деген қажеттілік туралы деректерді жалпылау, осы құралдарды дайындауға арналған өтінімдерді жасау бойынша жұмысқа басшылық жасайды, оларды алуды және қорғау объектілері арасында бөлуді ұйымдастырады;

3.1.14. Ақпараттың тиімділігін арттыру мақсатында озық тәжірибені таратуға және ақпаратты қорғаудың қазіргі заманғы ұйымдастырушылық-техникалық шараларын, құралдарын және тәсілдерін ендіруге ықпал жасайды;

3.1.15. Ақпаратты қорғауға қатысты мәселелерді шешу кезінде нормативтік-техникалық құжаттама талаптарының орындалуын, жұмыстарды орындаудың белгіленген тәртібінің, сондай-ақ қолданыстағы заңнаманың сақталуын бақылауды қамтамасыз етеді;

3.1.16. Экономикалық қызмет саласындағы, ұйымдағы ақпаратты қорғау бойынша бөлімшелер мен мамандардың қызметін үйлестіреді;

3.1.17. Персоналға құпия ақпаратты қорғауды оқытуды ұйымдастырады.

3.2. Бағыныштылығы:

3.2.1. Цифрлық даму орталығының ақпаратты қорғау жөніндегі бас маманы басқарма төрағасы – ректордың бұйрығымен қызметке тағайындалады және босатылады;

3.2.2. Цифрлық даму орталығының ақпаратты қорғау жөніндегі бас маманы тікелей Цифрлық даму орталығының директорына бағынады;

3.3. Цифрлық даму орталығының ақпаратты қорғау жөніндегі бас маманы білуі міндетті:

3.3.1. Мемлекеттік құпияларға, ақпаратты қорғауды қамтамасыз етуге қатысты заңнамалық, өзге де нормативтік құқықтық актілері және әдістемелік, нормативтік-техникалық материалдар;

3.3.2. Ұйымның және оның бөлімшелерінің даму перспективалары, мамандануы және қызметінің бағыттары, бөлімшелердің зерттеулер мен әзірлемелер процесіндегі өзара іс-қимыл жасау сипаты және қызметтік ақпараттың өту тәртібі;

3.3.3. Экономикалық қызмет түрінде, ұйымда қолданылып жүрген ақпаратты кешенді қорғауды ұйымдастыру жүйесі;

3.3.4. Ақпаратты қорғаудың техникалық және бағдарламалық-математикалық құралдарын дамытудың перспективалары мен бағыттары;

3.3.5. Қорғалатын мәліметтерді бақылау әдістері мен құралдарын ақпараттың жария болып қалу арналарын анықтау;

3.3.6. Техникалық барлауды ұйымдастыру;

3.3.7. Ғылыми зерттеулер, әзірлемелер жүргізуді, ақпаратты қорғау бойынша жұмыстарды орындауды жоспарлау және ұйымдастыру әдістері;

3.3.8. Арнайы зерттеулер мен тексерулерді, ақпаратты өткізудің, өңдеудің, көрсетудің және сақтаудың техникалық құралдарын қорғау бойынша жұмыстарды жүргізу шарттарын жасау тәртібі;

3.3.9. Осы лауазымдық нұсқаулық;

3.3.10. Еңбек заңнамасының негіздері;

3.3.11. Еңбекті қорғау, қауіпсіздік техникасы және өртке қарсы қауіпсіздік ережелері мен нормалары.

3.4. Біліктілік талаптары:

- 3.4.1. Тиісті мамандық бойынша жоғары білім (техникалық, инженерлік-экономикалық) және тиісті мамандық бойынша кем дегенде 3 жыл еңбек өтілі болуы;
- 3.4.2. Лауазымдық міндеттерге кіретін барлық мәселелерді толық білуі керек;
- 3.4.3. Өз біліктілігін үнемі арттырып отыруға тиіс.

4. Жауапкершілігі және құқығы

4.1. Цифрлық даму орталығының ақпаратты қорғау жөніндегі бас маманы жауапты:

4.1.1. Қазақстан Республикасының қолданыстағы еңбек заңнамасында белгіленген шекте осы лауазымдық нұсқаулықта көзделген өзінің лауазымдық міндеттерін тиісінше емес орындағаны немесе орындамағаны үшін;

4.1.2. Қазақстан Республикасының қолданыстағы әкімшілік, қылмыстық және азаматтық заңнамасында белгіленген шектерде өз қызметі процесінде жасалған құқық бұзушылықтар үшін;

4.1.3. Қазақстан Республикасының қолданыстағы Еңбек және азаматтық заңнамасында белгіленген шекте ұйымға материалдық залал келтіргені үшін.

4.2. Цифрлық даму орталығының ақпаратты қорғау жөніндегі бас маманы өкілетті:

4.2.1. Цифрлық даму орталығының қызметіне қатысты жобаларын әзірлеуге қатысу.

4.3. Цифрлық даму орталығының ақпаратты қорғау жөніндегі бас маманы құқылы:

4.3.1. Өз әзірлемелеріне авторлық құқық орнатуға;

4.3.2. Авторлық әзірлемелер ретінде өзінің жеке портфолиосына көркемдік - дизайнерлік шешімдерді санауға;

4.3.3. Ұйым басшылығынан лауазымдық міндеттерін орындау үшін қажетті ұйымдастырушылық-техникалық жағдайларды (оның ішінде ыңғайлы жұмыс орны, заманауи жұмыс компьютері, жеткілікті жылдам әрекет ету және жарақтандыру, қажетті бағдарламалық қамтамасыз ету, интернет желісіне бөлінген қолжетімділік) қамтамасыз етуді талап ету;

4.3.4. Тікелей басшыдан және жоғары тұрған басшылықтан міндеттерді, функцияларды және лауазымдық міндеттерді орындауға жәрдем көрсетуді талап етуге;

4.3.5. Атқаратын лауазымы бойынша оның құқықтары мен міндеттерін, лауазымдық міндеттерін орындау сапасын бағалау өлшемшарттарын айқындайтын құжаттармен танысуға құқылы;

4.3.6. Ұйым басшылығының қарауына осы лауазымдық нұсқаулықта көзделген міндеттерге байланысты жұмысты жетілдіру бойынша ұсыныстар енгізуге;

4.3.7. Бөлінген бюджет аясында қажетті әдебиеттер мен мамандандырылған бағдарламалық қамтамасыз етуді сатып алуға.

5. Сілтемелер

1. ҚР Еңбек кодексі 23.11.2015 ж. № 414-V;
2. "Білім туралы" ҚР Заңы;
3. 2011 жылғы 18 ақпандағы "Ғылым туралы" ҚР Заңы. № 407-IV;
4. ҚР «Сыбайлас жемқорлыққа қарсы іс-қимыл туралы» заңы 18.11.2015 ж. № 410-V;
5. СТ РК ИСО 9001-2016 Сапа менеджменті жүйелері. Талаптар;
6. ҚР БҒМ 2011 жылғы 20 сәуірдегі № 152 бұйрығы Кредиттік оқыту технологиясы бойынша оқу процесін ұйымдастыру қағидаларын бекіту туралы;

7. Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университетінің жарғысы;
8. СМК.08.ПД.28 Академиялық саясат;
9. СМК.08.ПД.06; Университеттің ішкі тәртіп ережелері;
10. Қызметкерлердің лауазымдық нұсқаулығы.

УТВЕРЖДАЮ
Председатель Правления, ректор
НАО «Западно-Казахстанский
аграрно-технический
университет имени Жангирдына»
А.М.Наметов
«10» _____ 2023 г.



ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
ГЛАВНОГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ
ЦЕНТРА ЦИФРОВОГО РАЗВИТИЯ

СМК.07.ДИ.196

Редакция № 00

Экземпляр № _____

Разработано: 04.05.2023г. Камалова Г.А.	Согласовано: 05.05.2023г. Таубаев У.Б.	Введено: 11.05.2023г. Впервые Пересмотр: 11.05.2026г.
	Алмагамбетова М.Ж.	
	Ихсанов Е.Б.	
	Таскалиев Е.К.	

1. Назначение

Настоящая инструкция разработана в соответствии с Трудовым кодексом и Законом «Об образовании» Республики Казахстан.

2. Применение

Настоящая инструкция действительна для главного специалиста по защите информации Центра цифрового развития.

3. Должностные обязанности

3.1. Главный специалист по защите информации обязан:

3.1.1. Исполняет свои обязанности под общим руководством первого руководителя организации и его заместителей и во взаимодействии с руководителями иных подразделений и служб;

3.1.2. В пределах своей компетенции осуществляет руководство деятельностью соответствующих структурных подразделений (служб) по направлению и координации работы подразделения, решает административные вопросы;

3.1.3. Руководит выполнением работ по комплексной защите информации в виде экономической деятельности, в организации, обеспечивая эффективное применение всех имеющихся организационных и технических мер в целях защиты секретных сведений и обеспечения режима секретности;

3.1.4. Участвует в разработке технической политики и определении перспектив развития технических средств контроля, организует разработку и внедрение новых технических и программно-математических средств защиты, исключающих или существенно затрудняющих несанкционированный доступ к секретной информации;

3.1.5. Участвует в рассмотрении технических заданий на проекты изделий, научно-исследовательские и опытно-конструкторские работы, подлежащие защите, осуществляет контроль над включением в них требований нормативно-технических и методических документов по защите информации и выполнением этих требований;

3.1.6. Готовит предложения для включения в планы и программы работ организационных и инженерно-технических мер по защите информационных систем;

3.1.7. Участвует в работе по созданию безопасных информационных технологий, отвечающих требованиям комплексной защиты информации;

3.1.8. Организует проведение научно-исследовательских работ в области совершенствования систем защиты информации и повышения их эффективности;

3.1.9. Выполняет весь комплекс (в том числе особо сложных) работ, связанных с контролем и защитой информации, на основе разработанных программ и методик;

3.1.10. Организует сбор и анализ материалов о возможных каналах утечки информации, в том числе по техническим каналам, при проведении исследований и разработок, связанных с созданием и производством специальных изделий (продукции), необходимых для проведения работ по обеспечению защиты информации;

3.1.11. Обеспечивает координацию проводимых организационно-технических мероприятий, разработку методических и нормативных материалов и оказание необходимой методической помощи в проведении работ по защите информации, оценке технико-экономической эффективности предлагаемых и реализуемых организационно-технических решений;

3.1.12. Организует работу по сбору и систематизации необходимой информации об объектах, подлежащих защите, и охраняемых сведениях, осуществляет методическое

руководство и контроль над работой по оценке технико-экономического уровня и эффективности разрабатываемых мер по защите информации.

3.1.13. Возглавляет работу по обобщению данных о потребности в технических и программно-математических средствах защиты информации, аппаратуре контроля, составлению заявок на изготовление этих средств, организует их получение и распределение между объектами защиты;

3.1.14. Содействует распространению передового опыта и внедрению современных организационно-технических мер, средств и способов защиты информации с целью повышения ее эффективности;

3.1.15. Обеспечивает контроль над выполнением требований нормативно-технической документации, за соблюдением установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты информации;

3.1.16. Координирует деятельность подразделений и специалистов по защите информации в виде экономической деятельности, в организации;

3.1.17. Организует обучение персонала по охране секретной информации.

3.2. Подчиненность:

3.2.1. Главный специалист по защите информации Центра цифрового развития назначается и освобождается от должности приказом председателя правления – ректора;

3.2.2. Главный специалист по защите информации Центра цифрового развития подчиняется непосредственно директору Центра цифрового развития;

3.3. Главный специалист по защите информации Центра цифрового развития должен знать:

3.3.1. Законодательные, иные нормативные правовые акты и методические, нормативно-технические материалы, касающиеся государственных секретов, обеспечения защиты информации;

3.3.2. Перспективы развития, специализацию и направления деятельности организации и их подразделений, характер взаимодействия подразделений в процессе исследований и разработок и порядок прохождения служебной информации;

3.3.3. Систему организации комплексной защиты информации, действующую в виде экономической деятельности, в организации;

3.3.4. Перспективы и направления развития технических и программно-математических средств защиты информации;

3.3.5. Методы и средства контроля охраняемых сведений, выявления каналов утечки информации;

3.3.6. Организацию технической разведки;

3.3.7. Методы планирования и организации проведения научных исследований, разработок, выполнения работ по защите информации;

3.3.8. Порядок заключения договоров на проведение специальных исследований и проверок, работ по защите технических средств передачи, обработки, отображения и хранения информации.

3.3.9. Отечественный и зарубежный опыт в области технической разведки и защиты информации;

3.3.10. Основы экономики, организации производства, труда и управления;

3.3.11. Трудовое законодательство, порядок внутреннего трудового распорядка, по безопасности и охране труда, производственной санитарии, требования пожарной безопасности.

- 3.3.12. Настоящую должностную инструкцию;
- 3.3.13. Основы трудового законодательства;
- 3.3.14. Правила и нормы охраны труда, техники безопасности и противопожарной безопасности.

3.4. Квалификационные требования:

- 3.4.1. Должен иметь высшее профессиональное (техническое, инженерно - экономическое) образование по соответствующей специальности и/или стаж работы в должности не менее 3 лет;
- 3.4.2. Должен обладать в полном объеме знанием всех вопросов, входящих в должностные обязанности;
- 3.4.3. Должен постоянно повышать свою квалификацию.

4. Ответственность и полномочия

4.1. Главный специалист по защите информации несет ответственность:

- 4.1.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, в пределах, установленных действующим трудовым законодательством Республики Казахстан;
- 4.1.2. За правонарушения, совершенные в процессе своей деятельности, - в пределах, установленных действующим административным, уголовным и гражданским законодательством Республики Казахстан;
- 4.1.3. За причинение материального ущерба организации - в пределах, установленных действующим трудовым и гражданским законодательством Республики Казахстан.

4.2. Главный специалист по защите информации Центра цифрового развития уполномочен:

- 4.2.1. Участвовать в разработке проектов Центра цифрового развития, касающихся его деятельности.

4.3. Главный специалист по защите информации Центра цифрового развития имеет право:

- 4.3.1. Устанавливать авторство на собственные разработки;
- 4.3.2. Зачитывать художественно-оформительские решения в свой личный портфолио как авторские разработки;
- 4.3.3. Устанавливать порядок и вид предоставления информации для размещения на веб-сервере;
- 4.3.4. Требовать от руководства организации обеспечения организационно-технических условий, необходимых для исполнения должностных обязанностей (в т.ч. удобное рабочее место, современный рабочий компьютер достаточного быстродействия и оснащения, необходимое программное обеспечение, выделенный доступ в сеть Интернет);
- 4.3.5. Требовать от непосредственного руководителя и вышестоящего руководства оказания содействия в выполнении задач, функций и должностных обязанностей;
- 4.3.6. Знакомиться с документами, определяющими его права и обязанности по занимаемой должности, критерии оценки качества исполнения должностных обязанностей;
- 4.3.7. Вносить на рассмотрение руководства организации предложения по совершенствованию работы, связанной с предусмотренными настоящей должностной инструкцией обязанностями;
- 4.3.8. В рамках выделенного бюджета приобретать необходимую литературу и специализированное программное обеспечение.

5. Ссылки

1. Трудовой кодекс РК от 23.11.2015 г. № 414-V;
2. Закон РК «Об образовании»;
3. Закон РК «О науке» от 18 февраля 2011 г. № 407-IV;
4. Закон РК «О противодействии коррупции» от 18 ноября 2015 г. № 410-V;
5. СТ РК ИСО 9001-2016 Системы менеджмента качества. Требования;
6. Приказ МОН РК от 20 апреля 2011 г. № 152 об утверждении Правил организации учебного процесса по кредитной технологии обучения;
7. Устав Западно-Казахстанского аграрно-технического университета имени Жангир хана;
8. СМК.08.ПД.28 Академическая политика;
9. СМК.08.ПД.06; Правила внутреннего распорядка университета;
10. Должностные инструкции сотрудников.