Академия развития профессиональных компетенций HR UP SKILL при участии ТОО «Контрольно-аналитическая служба РЕВИЗОР»

781120kz@mail.ru | hrdelo_kz | web-akademia.com | +7 777 428 97 11

ИС «КАБИНЕТ КАДРОВИКА» 2026 г.

Автор: Екатерина Лебедь, материалы разрешено использовать исключительно для личных целей.

ПРАКТИЧЕСКИЙ КОНСПЕКТ.

КИБЕРБЕЗОПАСНОСТЬ НА ПРАКТИКЕ

Как одна ссылка в рабочем чате превращается в угнанный аккаунт: правила для работы, для себя и для своей семьи.

Примечание к конспекту. Материал основан на прямом эфире, проведенном после фишинговой атаки на профессиональную группу «Кадровики Казахстана».

В конспекте — реальные схемы мошенников, пошаговые настройки Telegram, WhatsApp и рабочего компьютера, действия при инциденте и комплект образцов документов работодателя.

Образцы показывают логику и не предназначены для копирования без адаптации: каждый документ нужно привести в соответствие с действующими процессами вашей организации и проверить по актуальной редакции законодательства.

Автор: Екатерина Лебедь

ИС «КАБИНЕТ КАДРОВИКА» КОНСПЕКТ ЭФИРА

Как одна ссылка в рабочем чате превращается в угнанный аккаунт. Правила для работы, для себя и для своей семьи.

Прямой эфир 4 ноября 2026 года. Автор — Екатерина Лебедь, юрист по трудовому праву РК, кадровый аудитор

КАК ПОЛЬЗОВАТЬСЯ ЭТИМ ПОСОБИЕМ (важное примечание автора):

Это пособие — авторский практический материал. В нем собраны нормы законодательства, реальные ситуации и образцы документов, которые показывают, как требования кибербезопасности могут работать в кадровой практике.

1. **Образцы — это пример, а не готовый документ.** Все приказы, требования, акты, записки и формы составлены для вымышленной компании ТОО «Достар-KZ». Они показывают логику: что включить, на какую норму опереться, как связать документ с реальным процессом. **Ваша компания устроена иначе:** другие системы, другие люди, другие доступы и другая структура управления. Поэтому каждый образец нужно адаптировать под ваши действующие бизнес-процессы, а не копировать целиком.
2. **Документ, скопированный «как есть», не защищает компанию.** Он создает видимость порядка, а при первой проверке, инциденте или споре показывает, что требования написаны не про вашу организацию. Документ работает только тогда, когда он отражает то, что у вас происходит на самом деле.
3. **Актуальность.** Материал подготовлен по законодательству Республики Казахстан по состоянию на ноябрь 2026 года: Трудовой кодекс РК — на 07.09.2026, КоАП РК — на 20.08.2026, Закон РК «О кибербезопасности» — на 12.07.2026. Законодательство меняется. Перед применением проверяйте действующую редакцию норм.
4. **Это не индивидуальная консультация.** Пособие носит информационный характер. Решения о применении материалов в конкретной организации принимает сама организация с учетом своих обстоятельств. Автор не несет ответственности за последствия использования материалов без адаптации к деятельности конкретного работодателя.
5. **Распространение.** Пособие является объектом авторского права. Я разрешаю свободно распространять его: пересылать коллегам, размещать в профессиональных сообществах, использовать для обучения и для работы в своей организации — при сохранении имени автора и без изменения содержания. **Использовать пособие или его части в коммерческой деятельности (продавать, включать в платные курсы, консультации, сборники) без моего письменного согласия запрещено**.

Пользуйтесь, делитесь с коллегами и внедряйте с умом. Я создавала этот материал для того, чтобы кибербезопасность в компаниях стала рабочей практикой, а не очередной скаченной из интернета папкой с документами.

С уважением, **Екатерина Лебедь,** юрист по трудовому праву РК, кадровый аудитор ИС «Кабинет кадровика», https://web-akademia.com/wpm/start, https://www.hrdok.kz/

1. Что теперь говорит Трудовой кодекс

§ ТК РК, пп. 3) п. 2 ст. 22 — работник обязан

соблюдать требования по безопасности и охране труда, пожарной безопасности, промышленной безопасности, **кибербезопасности** и производственной санитарии на рабочем месте.

§ ТК РК, пп. 25-1) п. 2 ст. 23 — работодатель обязан

ознакомить работников с требованиями актов работодателя по соблюдению требований кибербезопасности и осуществлять внутренний контроль за их исполнением.

Обе нормы действуют с 25 августа 2026 года (Закон РК от 24.06.2026 № 326-VIII). Рядом осталась прежняя обязанность работодателя — осуществлять сбор, обработку и защиту персональных данных работника (пп. 24) п. 2 ст. 23 ТК РК).

Важное разъяснение

Письмо Министерства труда и социальной защиты населения РК от 17.09.2026 № ЖТ-2026-03677189: **отсутствие у работодателя отдельного акта по вопросам кибербезопасности не является нарушением пп. 25-1) п. 2 ст. 23 ТК РК.**

То есть «срочно скачайте положение» — не требование закона. Требования можно включить в действующие акты: правила трудового распорядка, положение о персональных данных, инструкцию по документообороту. Важно, чтобы они были конкретными, работник был с ними ознакомлен, а исполнение проверялось.

ПОЗИЦИЯ АВТОРА

Все лето и осень профессиональные чаты обменивались положениями и приказами о кибербезопасности. А когда пришла настоящая проверка — атака в рабочей группе, — сработали не документы, а привычки. Документ сам по себе не защищает. Защищает привычка остановиться и проверить.

Настраивать сети, серверы и программы — задача ИТ-специалистов, а не кадровика. Кадровик отвечает за свой участок: свой аккаунт, свою ЭЦП, данные работников, которые у него в руках, и ознакомление работников с требованиями работодателя.

2. Что случилось в группе «Кадровики Казахстана»

ПРИМЕРНЫЙ ОБРАЗЕЦ

Сообщение, которое пришло в группу

Участник группы через **@TG_AUTH_ROBOT**

‼ Чат переносится в новую группу. Нажмите на этот текст, чтобы перейти в нее.

💬 Затем нажмите кнопку «Начать», чтобы присоединиться к группе.

📌 Закреплено

Факт	Что произошло
Кто отправлял	Аккаунты давних участников группы — тех, кому доверяют годами. Не администратор и не владелец группы
Сколько длилось	Около 24 часов: от первых сообщений вечером 29 октября до остановки рассылки
Масштаб	Около 10 аккаунтов разослали сообщение и вышли из группы за полтора часа утром 30 октября
Последствия	Два аккаунта к вечеру стали «Удаленный аккаунт», у одного появилось случайное имя. Бот-модератор на следующий день пометил один из аккаунтов как спамерский

Расчет сделан по журналу модерации группы. Имена участников не раскрываются.

3. Как устроена схема: это не взлом

1. Сообщение «Чат переносится» приходит от знакомого человека.
2. Ссылка t.me открывает окно прямо внутри Telegram — бот или мини-приложение.
3. Окно просит ввести код, который Telegram прислал вам.
4. Код введен — устройство мошенников вошло в ваш аккаунт.

> **Главное**
> Ни вируса, ни подбора пароля. Человек сам нажимает «разрешить» и сам отдает вход в свой аккаунт. Схему описала «Лаборатория Касперского» 11 февраля 2026 года.

Боты, через которые шла рассылка

Адрес	Как распознать
@TG_AUTH_ROBOT, @AuthGateApp, @TelegaAuthApp	**Auth** — authorization, вход в аккаунт. Чтобы перейти в новый чат, ничего «авторизовать» не нужно
t.me/…_bot?startapp=…	**startapp** — откроется приложение, а не группа

Боты-модераторы такие сообщения не поймали: обычная ссылка t.me, ни одного рекламного слова, писали давние участники. Фильтр ловит спам, а фишинг рассчитан на человека.

Что бывает с захваченным аккаунтом

Последствие	Как это выглядит
Рассылка от вашего имени	По всем группам и чатам — как и было у нас

Последствие	Как это выглядит
Сообщения близким	«Срочно займи», «переведи на Kaspi», «проголосуй за племянницу» — с вашей фотографией
Ваши переписки и файлы	Фото удостоверения, справки, рабочие документы с ИИН работников, пересланные «на минутку»
Вас выкинут из аккаунта	Мошенники завершат ваши сеансы и поставят свой облачный пароль
Черные списки	Аккаунт помечают как спамерский, путь в группы закрывается
Потеря доверия	Коллеги и клиенты видят мошенническую рассылку от вашего имени

Признаки, что аккаунтом пользуется кто-то еще

- Вам пишут: «Ты мне прислал странную ссылку».
- В «Устройствах» есть вход, которого вы не делали, или пришло уведомление о новом входе.
- Вы «вышли» из групп, из которых не выходили.
- Изменились имя пользователя, фото или описание.
- В отправленных есть сообщения, которых вы не писали.
- Вас выбросило из аккаунта, хотя вы ничего не делали.

4. Почему нажимают даже опытные специалисты

Причина	Как работает
Знакомая среда	Сообщение пришло в рабочую группу, которой доверяешь годами
Ложный авторитет	Похоже на объявление администрации
Срочность	Не перейдешь сейчас — потеряешь доступ к группе
Привычка	Мы подтверждаем коды по десять раз на дню: eGov, 1414, банк, Enbek.kz

> **Главное**
> Это не про глупость. Мошенники добиваются, чтобы решение было принято раньше, чем человек успеет подумать. «Кто сильно торопит, тот готов ждать» — если вас торопят, срочности, скорее всего, нет.

5. Реальные схемы 2025–2026 годов

Когда и кто сообщил	Схема
9 июня 2026 Генпрокуратура	«Служба поддержки Telegram»: аккаунт удалят через 24 часа, для отмены введите код. Процедуры отмены удаления не существует
13 июля 2026 МВД	Фейковый аккаунт «директора» с настоящим фото просит бухгалтера срочно оплатить счет и никому не говорить
10 августа 2026 МВД	Массовые взломы WhatsApp. МВД советует включить двухэтапную проверку и проверить «Связанные устройства»
10 сентября 2026 Генпрокуратура	Мошенники представляются сотрудниками eGov

По данным Генеральной прокуратуры, ущерб от интернет-мошенничества в 2025 году — 12,2 млрд тенге. Вернуть удалось 5 млрд тенге.

«Курьер Kaspi» просит код, а SMS — от Aitu Passport

Звонят, когда вы ждете доставку: «курьер», «приеду через час», «назовите код». Код приходит не от 1414, а от Aitu Passport.

Это вход в цифровые госуслуги и облачная ЭЦП для подписания документов. Продиктовали код — мошенник входит в ваш цифровой профиль и может подписывать от вашего имени. В самой SMS написано: «Никому не говорите код».

Вывод. Курьеру код нужен только в момент передачи посылки (отправления). Курьеру код приходит в приложение магазина, например, Kaspi. Но точно НЕ в egov! Не знаете, от чего код, — не называйте его.

«Срок действия ЭЦП закончился. Нажмите 1»

Звонит робот «от eGov»: срок ЭЦП истек, для продления нажмите 1.

Дальше «оператор» просит код из SMS, пароль от ЭЦП или установить приложение. Официальный аккаунт eGov.kz ответил: сотрудники первыми с пользователями не связываются, это мошенники.

Вывод. Положите трубку. ЭЦП по телефону не продлевают. Срок проверьте сами, новый ключ выпускайте сами — в eGov Mobile или на pki.gov.kz.

Как проверить свои ключи ЭЦП в кабинете НУЦ

1. Откройте сайт НУЦ РК pki.gov.kz и найдите «Личный кабинет».
2. Войдите своей действующей ЭЦП: выберите ключ, введите пароль.
3. Откройте список сертификатов: там все ключи, которые выпускались на ваше имя, — действующие, истекшие и отозванные.

4. Видите ключ, который вы не выпускали или не помните, — отзовите его. Новый ключ выпустить быстрее, чем разбираться с последствиями чужой подписи.
5. Пользуйтесь только тем ключом, который хранится у вас и не скомпрометирован: никто не видел пароль, не копировал файл, носитель не оставался без присмотра.

Кабинет НУЦ есть и у физических, и у юридических лиц. Подробный разбор — в материалах «Кабинета кадровика» и на вебинаре №41.

6. Код из SMS или Telegram — это ключ от вашей двери

✓ Вводить можно	✕ Нельзя никогда
Только в то приложение или на тот сайт, который вы сами открыли, чтобы войти. Например: вы ставите Telegram на новый телефон, и он просит код	В окне бота или мини-приложения; на сайте по ссылке из сообщения; диктовать «банку», «курьеру», «оператору eGov»; пересылать кому-то в мессенджере

> **Правило**
> Кто просит ваш код — тот вор. Даже если он звонит от имени банка или полиции.

Пять вопросов перед любым переходом по ссылке

1. Кто именно просит и откуда я это знаю?
2. Почему это нужно сделать именно сейчас? Чтобы что?
3. Совпадает ли адрес с официальным?
4. Что я подтверждаю этим действием: передаю данные, деньги, доступ?
5. Могу ли я проверить это сам, не по этой ссылке?

Неясен хотя бы один ответ — не нажимайте. Откройте сервис сами или позвоните человеку. Сомнительную ссылку можно вставить в поисковую строку браузера или попросить проверить нейросеть, которой вы пользуетесь, — не переходя по ней.

> **Схема «собеседование в Zoom»**
> Вам предлагают работу или заказ, назначают онлайн-встречу. Ваша ссылка «не открывается», присылают скриншоты черного экрана, а потом — «нашу» ссылку на Zoom. Это подмененная страница: переход по ней может установить вредоносную программу или открыть доступ к уведомлениям.
> **Что делать.** Для разговора хватит видеозвонка в Telegram или WhatsApp — без новых программ. Чужую ссылку на «конференцию» сначала проверьте.

7. Найдите подвох

Сообщение	Подвох	Что делать
SMS «Kaspi.kz»: «Ваш Kaspi Gold будет заблокирован через 2 часа. Подтвердите данные по ссылке kaspi-gold-bezopasnost.com»	Срочность «через 2 часа»; адрес не kaspi.kz; просят «подтвердить данные» по ссылке	Ссылку не открывать. Откройте приложение банка сами или позвоните по номеру на карте
WhatsApp с нового номера: «Мама, привет! Телефон утопил, это мой новый номер. Срочно нужно 45 000 ₸, скинь на Kaspi, вечером объясню»	Новый номер, голоса нет; срочно нужны деньги; «объясню потом» — не дают время проверить	Позвонить на старый номер голосом. Спросить кодовое слово семьи
«Служба поддержки Telegram»: «Поступил запрос на удаление аккаунта. Отменить можно в течение 24 часов — нажмите и введите код»	Процедуры отмены удаления нет; просят код — это вход в аккаунт; давят страхом и сроком	Ничего не нажимать. Проверить «Настройки» → «Устройства»
Telegram «Директор» с настоящим фото: «Срочно оплатите счет поставщику по новым реквизитам. Я на совещании, не звоните, никому не говорите». Файл «Счет_118.pdf.exe»	«Не звоните», «никому не говорите»; новые реквизиты; .exe — это программа, а не документ	Ничего не оплачивать, файл не открывать. Перезвонить руководителю по известному номеру

8. Настройки, которые нужно сделать сегодня

НАСТРОИМ ВАШ TELEGRAM

Что	Где	Зачем
Облачный пароль	«Настройки» → «Конфиденциальность» → «Облачный пароль» → «Задать пароль». Укажите почту для восстановления и подтвердите ее кодом из письма	Без пароля код из SMS бесполезен для мошенника
Устройства	«Настройки» → «Устройства». Незнакомое устройство → «Завершить сеанс». Не уверены — «Завершить все другие сеансы». Внизу — «Автоматически завершать сеансы»	Видно, кто еще сидит в вашем аккаунте

Что	Где	Зачем
Номер телефона	«Конфиденциальность» → «Номер телефона» → «Никто»; «Кто может найти меня по номеру» → «Мои контакты»	Номер не видят в группах
Группы и каналы	«Конфиденциальность» → «Группы и каналы» → «Мои контакты»	Чужие не добавят в мошеннические чаты
Звонки	«Конфиденциальность» → «Звонки» → «Мои контакты»	«Служба безопасности банка» не дозвонится через Telegram

Из личного опыта автора

Облачный пароль — новый, которого нет больше нигде. Запишите его на бумаге и храните дома.

При первом вводе пароль можно показать значком «глаз», при повторном вводе — нет. Вводите посимвольно по записи, чтобы не ошибиться.

В некоторых версиях пункт называется «Двухэтапная аутентификация».

НАСТРОИМ ВАШ WHATSAPP

Что	Где
Двухэтапная проверка	«Настройки» → «Аккаунт» → «Двухэтапная проверка» → «Включить». PIN-код из 6 цифр, не дата рождения, и e-mail для восстановления
Связанные устройства	«Настройки» → «Связанные устройства». Незнакомый компьютер → «Выйти»
Группы	«Конфиденциальность» → «Группы» → «Мои контакты»
Звонки	«Конфиденциальность» → «Звонки» → «Заглушать неизвестные номера»
Код из SMS	Никому не пересылать 6-значный код WhatsApp — даже «другу», которому он «случайно пришел»

Названия пунктов на iPhone, Android и компьютере могут немного отличаться. Настройте то же самое родителям: они чаще всего общаются именно в WhatsApp.

9. Уже нажали: что делать сразу

Только открыл ссылку	Ввел код	Не могу войти в аккаунт
1. Закройте окно. 2. В боте ничего не нажимайте: ни «Начать», ни «Подтвердить». 3. Чат с ботом → «Остановить и заблокировать». 4. Проверьте «Устройства».	1. Сразу: «Настройки» → «Устройства» → «Завершить все другие сеансы». 2. Включите облачный пароль. 3. Напишите в группы и близким: «Мой аккаунт взломали, ссылки от меня не открывайте». 4. Удалите сообщения, отправленные от вашего имени.	1. Войдите заново по номеру телефона: код придет в SMS или в Telegram на другом устройстве. 2. Не получается — поддержка telegram.org/support. 3. Предупредите контакты звонком или в WhatsApp. 4. Сообщите администраторам групп.

Деньги и ЭЦП

Перевели деньги или назвали данные карты — сразу звоните в банк и в полицию: **102**.

Ввели пароль от ЭЦП на чужом сайте — отзовите сертификат и выпустите новый в НУЦ РК.

Короткие номера крупных банков

Kaspi Bank	9999
Halyk Bank (Народный банк)	7111 (физлица), 9595 (юрлица)
Jusan Bank	7711
Freedom Bank	595
ForteBank	7575
Банк ЦентрКредит (БЦК)	505
Отбасы банк	300
Bank RBK	7888
Bereke Bank	5030 (физлица), 7744 (юрлица)

10. Правила на каждый день для всей семьи

Ситуация	Правило
Звонок «из банка», «из полиции», «из eGov»	Положите трубку. Перезвоните сами по номеру на карте или на официальном сайте

Ситуация	Правило
Коды из SMS, 1414, eGov	Никому и никогда: ни «курьеру», ни «оператору», ни «сотруднику банка»
Приложения	Только из App Store и Google Play. Файл .apk из мессенджера не устанавливать
Ссылки в SMS и QR-коды	Не открывать. Адрес банка или eGov набирать самим
Фото документов	Не отправлять фото удостоверения в мессенджерах «для проверки»
Пароли	Разные для почты, eGov, банка и мессенджеров. Везде, где можно, — облачный пароль или вход в два шага

Защитите родителей и детей

- **Кодовое слово семьи** — вопрос, ответ на который знают только свои. Пишет «сын» с нового номера — спросите его. Голос сегодня тоже подделывают.
- **Правило «перезвони»** — любая просьба о деньгах только после звонка голосом на старый номер.
- **Лимит на переводы** в банковском приложении родителей.
- **Облачный пароль и двухэтапная проверка** родителям — настройте сами, пароль запишите и храните у них дома.
- **Детям и себе:** не выкладывать фото документов, билетов, школы с адресом, не показывать в реальном времени, где вы находитесь.

11. Схемы, которые бьют именно по кадровику и бухгалтеру

У кадровой службы и бухгалтерии есть то, что нужно мошенникам: персональные данные, ЭЦП организации, доступ к деньгам. Поэтому против них работают отдельные схемы. Ниже — каждая с порядком действий.

11.1. «Перечислите мою зарплату на новую карту»

Как выглядит

Бухгалтеру или кадровику приходит сообщение в мессенджере или письмо: «Здравствуйте, это Айгуль Серикова из отдела продаж. Поменяла банк, прошу с этого месяца перечислять зарплату на новую карту, номер такой-то. Заявление занесу потом». Сообщение может прийти с настоящего аккаунта коллеги, с ее фотографией и в ее манере письма, потому что аккаунт угнан.

Почему звонка работнику недостаточно. Звонок по номеру из личного дела — это уже лучше, чем ответ в том же чате, но он не доказывает, что на том конце именно работник: голос сегодня подделывают по записям из соцсетей и голосовых сообщений;

мошенники перевыпускают SIM-карту на свое устройство по поддельной доверенности; телефон могли украсть вместе с доступом к мессенджеру; номер в личном деле мог устареть.

Поэтому личность подтверждают не одним звонком, а документами и независимым каналом.

Правило. Реквизиты для перечисления заработной платы меняются только по заявлению самого работника, подписанному лично или его ЭЦП, и только на счет, открытый на его имя.

Шаг	Что сделать	Зачем
1. Не отвечать в том же канале	Сообщение или письмо о смене реквизитов не исполняется. Ответ: «Реквизиты меняются только по личному заявлению»	Если аккаунт угнан, мошенник не получит подтверждения и подсказок
2. Заявление	Принимается: лично в кадровой службе, с предъявлением удостоверения личности; или в электронном виде с ЭЦП работника — физического лица через систему электронного документооборота. Скан, фото, сообщение в мессенджере заявлением не являются	ЭЦП и личное присутствие подтверждают личность, сообщение — нет
3. Подтверждение через руководителя	Непосредственный руководитель работника подтверждает, что работник лично знает о заявлении. Для дистанционного работника — только заявление с ЭЦП	Независимый канал: мошенник не контролирует одновременно аккаунт работника и его руководителя
4. Документ банка	Справка банка о реквизитах счета, в которой указаны ФИО и ИИН владельца. ИИН сверяется с личным делом. Счет другого лица не принимается	Деньги уходят только на счет работника
5. Срок	Новые реквизиты применяются с ближайшей выплаты после проверки. Просьба «нужно уже сегодня» — повод для дополнительной проверки, а не для спешки	Срочность — главный признак мошенничества
6. Уведомление работника	После изменения работник получает уведомление лично или по корпоративной почте: «Реквизиты изменены по вашему заявлению от …»	Если работник заявление не подавал, он узнает сразу, а не в день зарплаты

Шаг	Что сделать	Зачем
7. Если просьба пришла в мессенджере	Сообщить работнику лично и ответственному за кибербезопасность: возможно, аккаунт работника угнан	Мошенник уже пишет от имени работника и другим людям

ПРИМЕРНЫЙ ОБРАЗЕЦ

ЗАЯВЛЕНИЕ

Директору ТОО «Достар-KZ» Нурмагамбетову А. С.
менеджера отдела продаж
Сериковой Айгуль Маратовны

Прошу с 1 декабря 2026 года перечислять мою заработную плату и иные выплаты на текущий счет, открытый на мое имя в АО «…», № KZ00 0000 0000 0000 0000, вместо ранее указанного счета.

Приложение: справка АО «…» о реквизитах счета от 20.11.2026 на 1 л.

_____ А. М. Серикова
20 ноября 2026 года

Отметки о проверке:

Личность заявителя установлена по удостоверению личности № _____.	Менеджер по персоналу _____ Ж. Б. Ермекова, 20.11.2026
Заявление подано работником лично, подтверждаю.	Руководитель отдела продаж _____ Р. К. Ахметов, 20.11.2026
ИИН владельца счета в справке банка совпадает с ИИН работника.	Бухгалтер _____ А. Б. Сейтенова, 20.11.2026
Работник уведомлен об изменении реквизитов 20.11.2026 по корпоративной почте или КЭДО.	Менеджер по персоналу _____ Ж. Б. Ермекова, 20.11.2026

ОБУЧЕНИЕ И ПОВЫШЕНИЕ КВАЛИФИКАЦИИ:
Все участки кадрового учета и кадровые процедуры с нуля и для систематизации учета компании — «Специалист отдела кадров»
https://www.hrdok.kz/ok2026

11.2. Резюме кандидата с «сюрпризом»

Кадровик открывает вложения от незнакомых людей каждый день — это его работа. Поэтому «резюме» — один из самых удобных способов доставить вредоносную программу на компьютер компании.

Признак	Почему опасно
Архив .zip или .rar, тем более с паролем «в тексте письма»	Антивирус не может проверить архив, к которому установлен пароль
Файл «Резюме_Иванова.pdf.exe», «.scr», «.lnk», «.js», «.bat»	Это программа, а не документ. Двойное расширение прячет настоящий файл
Документ Word просит «Включить содержимое» или «Разрешить редактирование», чтобы «увидеть резюме»	Так запускаются макросы — вредоносный код внутри документа
Ссылка «резюме на Google Диске», после которой просят войти в почту	Страница-двойник крадет пароль от вашей почты
Кандидат торопит: «Откройте срочно, у меня еще два оффера»	Срочность — главный признак манипуляции

Как безопасно работать с резюме

1. Включите показ расширений файлов. Windows: «Проводник» → «Вид» → «Показать» → «Расширения имен файлов». Теперь «Резюме.pdf.exe» не притворится PDF.
2. Принимайте резюме в формате PDF или DOCX — через сайт вакансий, форму на сайте компании или рабочую почту. В объявлении о вакансии так и напишите.
3. Перед открытием — проверка антивирусом: правой кнопкой по файлу → «Проверить с помощью…».
4. Документы из неизвестного источника открывайте в режиме просмотра: защищенный просмотр Word, предпросмотр в почте или браузере. Кнопку «Включить содержимое» не нажимайте никогда.
5. Архивы с паролем и исполняемые файлы от кандидатов не открывайте. Вежливый ответ: «Пришлите, пожалуйста, резюме в формате PDF».
6. По ссылке на резюме не вводите пароль от своей почты. Настоящий документ открывается без входа в ваш аккаунт.

11.3. «Звонят из налоговой» или «из трудовой инспекции»

Это не теория. Комитет государственных доходов в 2025–2026 годах несколько раз предупреждал о мошенниках, которые звонят от имени налоговых органов. Легенды: «нет отчетности по форме 270, заблокируем счета», «вы в списках финансового мониторинга», «нужно подтвердить вид деятельности в приложении», «пройдите верификацию».

§ Разъяснение КГД МФ РК (по сообщениям zakon.kz, 03.11.2025; digitalbusiness.kz, 12.05.2026)

Органы государственных доходов **не направляют уведомления на электронную почту, в WhatsApp или Telegram**, не запрашивают ЭЦП, коды подтверждения, реквизиты карт, пароли и не требуют по телефону устанавливать приложения.

Официальное информирование — через кабинет налогоплательщика на eGov.kz и kgd.gov.kz, официальные письма в системе электронного документооборота и контакт-центр **1414**.

Вам говорят	Что сделать
«Оплатите штраф по ссылке / на карту»	Штраф уплачивается только на основании постановления, в бюджет, по реквизитам из постановления. Никаких карт и ссылок
«Срочно пришлите документы в WhatsApp, у вас проверка»	Проверка оформляется официально, документы запрашиваются официальным запросом. Попросите письменный запрос и перезвоните в орган по номеру с официального сайта
«Установите приложение для верификации»	Положить трубку. Официальные приложения скачиваются только из App Store и Google Play по ссылке с сайта госоргана
«Назовите код из SMS»	Положить трубку. Это вход в ваш кабинет или ЭЦП

Для трудовых инспекций в Казахстане такие звонки пока не стали массовыми, но схема та же. Минтруда уже опровергало рассылки в мессенджерах о «массовых проверках работодателей» по Enbek.kz.

11.4. «Дайте данные работника» по телефону

Как выглядит

«Здравствуйте, это банк / МФО / служба безопасности. Подтвердите, что Касымов Ержан работает у вас, назовите его должность и доход». Или «я его родственник, продиктуйте его ИИН и адрес».

- Сведения о работнике по телефону не сообщаются никому: ни «банку», ни «родственнику», ни «следователю».
- Справку с места работы выдают **самому работнику** по его письменному заявлению. Банк проверяет доход по сведениям из государственных источников и справке, которую принес работник.
- Запрос госоргана — только письменный, с указанием основания. Ответ — тоже письменно, на официальный адрес органа.

- Персональные данные работника передаются третьим лицам только с его согласия или в случаях, прямо установленных законом (законодательство о персональных данных и их защите).

11.5. Письма «от Enbek.kz», «ЕСУТД», «НУЦ»

Признак фишинга	Как на самом деле
«Ваша ЭЦП истекает, обновите по ссылке»	Новый ключ выпускается только на pki.gov.kz или в eGov Mobile. Ссылки в письмах не нужны
«Подтвердите сведения ЕСУТД, иначе штраф»	Сведения вносятся в кабинете работодателя на Enbek.kz, в который вы входите сами
Адрес похож на настоящий: enbek-kz.com, egov-kz.org	Официальные адреса: enbek.kz, egov.kz, pki.gov.kz, kgd.gov.kz — проверяйте каждую букву
Просят ввести пароль от ЭЦП на странице	Пароль от ЭЦП вводится только в окне программы NCALayer на официальном сайте

12. Договоритесь о платежных коммуникациях

Схема «директор срочно просит оплатить, не звоните, никому не говорите» работает только там, где деньги можно отправить по одному сообщению. Если в компании письменно установлен порядок оплат, мошеннику просто не за что зацепиться: бухгалтер не нарушает распоряжение руководителя, а исполняет утвержденный порядок.

> **Главная мысль**
>
> Ни один руководитель не отправляет требование оплатить по новым реквизитам и «уходит на совещание». Оплата — это всегда договор, счет, сумма и согласование по известному каналу. Договоритесь об этом с руководителем заранее — письменно.

ПРИМЕРНЫЙ ОБРАЗЕЦ

ПОРЯДОК СОГЛАСОВАНИЯ И ПРОВЕДЕНИЯ ПЛАТЕЖЕЙ
(ключевые пункты)

1. Платежи поставщикам и подрядчикам проводятся только на основании заключенного договора и счета, зарегистрированных в журнале входящих документов.
2. Реквизиты получателя берутся из договора. Изменение реквизитов принимается только по официальному письму контрагента на бланке за подписью руководителя и подтверждается звонком бухгалтера контактному лицу **по телефону, указанному в договоре**, а не в письме.
3. Распоряжение об оплате директор дает письменно: подписью на счете, в системе электронного документооборота или с рабочей электронной почты. Сообщения в мессенджерах, голосовые сообщения и звонки распоряжением об оплате не являются.

4. Плановые платежи проводятся по вторникам и четвергам. Срочный платеж вне этих дней — только после личного или телефонного подтверждения директора по известному номеру.
5. Работник, получивший требование оплатить «срочно», «по новым реквизитам», «никому не говоря», платеж не проводит и сообщает ответственному за кибербезопасность.
6. Исполнение пунктов 1–5 не может рассматриваться как неисполнение распоряжения руководителя.

Пункт 6 защищает бухгалтера: отказ провести «срочный платеж» по сообщению в мессенджере — это соблюдение утвержденного порядка, а не нарушение трудовой дисциплины.

13. Защитите себя: кредиты, SIM-карта, кредитная история

13.1. «Стоп-кредит»: добровольный отказ от займов

Любой гражданин может сам установить запрет на получение банковских займов и микрокредитов на свое имя. После подключения в кредитной истории появляется отметка, банки и МФО видят ее при запросе в кредитное бюро и должны отказать в займе. Раньше отказ действовал 6 месяцев, теперь его можно установить бессрочно.

Где	Как
Портал eGov.kz	Войти в личный кабинет → «Сервисы» → «Добровольный отказ от получения банковских займов, микрокредитов» → «Заказать услугу онлайн» → заполнить форму → подписать ЭЦП. Результат — в «Истории получения услуг»
eGov Mobile	«Услуги» → «Налоги и финансы» → «Добровольный отказ от получения кредитов» → заполнить → подтвердить

Нужен кредит самому — отказ снимают тем же способом, а после получения займа устанавливают снова. Это особенно важно для пожилых родителей.

13.2. Кредитная история: проверять раз в квартал

Где	Как и сколько стоит
eGov.kz	Услуга получения персонального кредитного отчета: войти → «Заказать услугу онлайн» → подписать ЭЦП. Отчет — в «Истории получения услуг». Через eGov услуга платная, около 400 тенге
Первое кредитное бюро (1cb.kz)	Сайт или приложение. Один полный персональный кредитный отчет в год — бесплатно
Государственное кредитное бюро	Сервис в eGov Mobile «ГКБ. ГИД кредитной и страховой истории» https://egov.kz/ru/services/presale/P1903 и сайт https://id.mkb.kz/#/auth

ПРОЕКТ «КАБИНЕТ КАДРОВИКА» — вебинары и разборы весь год,
https://www.hrdok.kz/kabinet

Что искать

Что смотреть в отчете: займы, которых вы не брали; запросы вашего отчета организациями, к которым вы не обращались. Нашли чужой заем — сразу в банк, выдавший его, и в полицию (102). Оспорить сведения можно онлайн.

13.3. ПИН-код на SIM-карту

Если телефон украли, вор вставит вашу SIM-карту в другой телефон и получит коды из SMS: от банка, eGov, Telegram. ПИН-код на SIM-карте это закрывает: без него карта не заработает ни в одном телефоне.

Телефон	Как включить
iPhone	«Настройки» → «Сотовая связь» → выберите SIM-карту → «SIM-PIN» → включить → ввести текущий ПИН-код. Затем там же «Изменить PIN» и задать свой
Android	«Настройки» → «Безопасность» (или «Биометрия и безопасность») → «Другие параметры безопасности» → «Блокировка SIM-карты» → включить → «Изменить PIN-код SIM-карты». Названия зависят от модели

Перед тем как включать

Заводской ПИН-код указан на пластиковой карточке, из которой выламывали SIM-карту. Нет карточки — уточните у оператора.

Три неверных попытки — SIM-карта блокируется, нужен PUK-код (тоже на карточке или у оператора). Поэтому новый ПИН запишите и храните дома вместе с облачным паролем.

После перезагрузки телефона ПИН будет запрашиваться каждый раз — это нормально.

14. Кибербезопасность как привычка в компании

При приеме на работу

1. Доступы — только по письменной заявке руководителя: какие системы, какие права, на какой срок.
2. Ознакомление с Требованиями по кибербезопасности — до начала работы, вместе с другими актами работодателя.
3. В первый день — 10 минут с ответственным: облачный пароль в рабочем мессенджере, 2FA в рабочей почте, Win + L, куда сообщать об инциденте.
4. Запись в акте ревизии учетных записей: что выдано и кем.

Ежемесячная пятиминутка

Привычка вырабатывается повторением, а не положением. Раз в месяц на планёрке или в рабочем чате — один реальный пример и одно конкретное действие. Пятиминутку ведёт ответственный за кибербезопасность. Кадровая служба помогает включить её в план планёрок.

> **Обратите внимание**
> Темы, касающиеся личных аккаунтов и финансов работников, даются как рекомендация: работодатель показывает, как защититься, но не проверяет личные аккаунты, кредитную историю и настройки телефонов работников.

Месяц	Тема пятиминутки
Январь	Что делать, если уже нажали: порядок действий и кому сообщать
Февраль	«Директор» в мессенджере просит срочно оплатить: разбор схемы
Март	Вложения в письмах: как увидеть, что «документ» на самом деле программа .exe
Апрель	Фишинговые письма и звонки «от КГД» и «от Enbek.kz»: как отличить настоящие
Май	Облачный пароль и устройства в Telegram, двухэтапная проверка в WhatsApp: где настройки
Июнь	Отпуск: фото билетов, документов и геолокация в соцсетях
Июль	Пароли: заменить самый старый, разные пароли для почты, банка и eGov
Август	2FA в рабочей почте: у всех ли включена
Сентябрь	Родительские и школьные чаты: ссылки «проголосуйте», «сдайте деньги»
Октябрь	ЭЦП: хранение носителя, проверка ключей в кабинете НУЦ
Ноябрь	Звонки «из банка» и «из полиции». «Стоп-кредит» как защита от займов на ваше имя
Декабрь	Предновогодние «акции», «подарки» и «доставки». Итоги года: какие инциденты были и что изменили

Пятиминутку не нужно оформлять протоколом. Достаточно, чтобы ответственный вёл короткий перечень проведённых тем: он пригодится в справке о внутреннем контроле (пункт 7 Требований по кибербезопасности).

Только тема августа касается рабочих систем, поэтому проверять её выполнение работодатель вправе. Остальные темы — рекомендации без контроля.

Учебная проверка

Раз в полгода ответственный за кибербезопасность отправляет работникам безобидное «фишинговое» письмо или сообщение и смотрит, кто нажмет и кто сообщит. Цель — не наказать, а показать на своем примере.

- Предусмотрите учебные проверки в Требованиях по кибербезопасности — чтобы они не стали неожиданностью.
- Результаты обсуждаются без имен: «нажали 4 человека из 14, сообщили 2».
- Тот, кто сообщил о подозрительном письме, — пример для всех. Тот, кто нажал, проходит пятиминутку повторно, без взысканий.

ОБУЧЕНИЕ И ПОВЫШЕНИЕ КВАЛИФИКАЦИИ:

Внутренний аудит соблюдения требований в своей компании — по каждой теме — «Управление трудовыми отношениями»

https://www.hrdok.kz/pravo-hr

15. Еще несколько схем, о которых стоит знать

Схема	Как защититься
QR-код на листовке, счетчике, парковке, в подъезде — ведет на поддельную страницу оплаты	Не сканировать QR из случайных мест. Оплачивать в приложении банка или на официальном сайте
Голос руководителя или родственника по телефону, сгенерированный по записям из соцсетей	Кодовое слово, перезвон на известный номер, порядок оплат — голос сам по себе ничего не доказывает
«Найденная» флешка у офиса или на парковке	Не вставлять в рабочий компьютер. Отдать ответственному
Бесплатный Wi-Fi в кафе, аэропорту	Не входить в банк, eGov, Enbek.kz и почту без мобильного интернета или VPN организации
Старый телефон или компьютер продают или отдают	Перед передачей — выйти из всех аккаунтов, удалить ЭЦП, сбросить до заводских настроек

16. Рабочий процесс: пошаговые инструкции

Правила «не передавать ЭЦП» и «не открывать .exe» работают, только когда превращаются в привычные действия. Ниже — то, что каждый кадровик, бухгалтер и юрист может настроить сам за один рабочий день.

Словарь: без этих слов инструкции не понять

1) **Учетная запись** — ваш «аккаунт» в системе: логин и способ входа (почта, Enbek.kz, банк-клиент, 1С, мессенджер).
2) **Аутентификация** — проверка, что входите именно вы.

3) **2FA** (от англ. two-factor authentication) — **двухфакторная аутентификация**: вход по двум признакам сразу. Первый — то, что вы знаете (пароль). Второй — то, что есть только у вас (код в приложении или SMS, ключ ЭЦП с паролем, отпечаток пальца). Украли пароль — без второго фактора войти все равно нельзя.
4) **Компрометация** — когда пароль, ключ ЭЦП или код мог стать известен постороннему: видели, сфотографировали, переслали, ввели на чужом сайте.
5) **Инцидент** — любое событие, которое угрожает данным или доступам: нажали подозрительную ссылку, потеряли флешку с ЭЦП, пришло уведомление о чужом входе.

16.1. Компьютер и экран

Действие	Как сделать	Зачем
Блокировать экран, уходя от стола	Windows: **Win + L** (Win — клавиша со значком окна). Mac: **Control + Command + Q**. Телефон — кнопка питания	Открытая почта, Enbek.kz или 1С становятся недоступны за секунду
Автоблокировка, если забыли	Windows: «Параметры» → «Персонализация» → «Экран блокировки» → «Заставка» → интервал 5 минут и отметка «Начинать с экрана входа в систему»	Компьютер сам закроется через 5 минут бездействия
Пароль на вход в компьютер	«Параметры» → «Учетные записи» → «Варианты входа». Пароль или ПИН-код, которые знаете только вы	Без пароля Win + L ничего не защищает
Обновления и антивирус	Не откладывать обновления Windows и не отключать антивирус «чтобы не мешал»	Старые версии программ — открытая дверь для вредоносных файлов

16.2. Пароли

Правило	Как выполнить
Длина — не меньше 12 символов	Используйте фразу из нескольких слов с цифрой и знаком: «Зима2026!ЧайСЛимоном». Ее легко запомнить и трудно подобрать
Уникальность	Для почты, eGov, банка, Enbek.kz, мессенджеров — разные пароли. Утек один — остальные целы

Правило	Как выполнить
Где хранить	В менеджере паролей с главным паролем или на бумаге дома. Не на стикере у монитора, не в файле «пароли.docx» на рабочем столе, не в заметках телефона без пароля
Когда менять	При подозрении на компрометацию, после увольнения работника, у которого был доступ, после передачи дел
Чего не делать	Не сохранять пароли в браузере на общем компьютере. Не диктовать пароль по телефону, даже «своему ИТ-специалисту»

16.3. Двухфакторная аутентификация (2FA): где включить

Сервис	Где включить	Второй фактор
Telegram	«Настройки» → «Конфиденциальность» → «Облачный пароль»	Облачный пароль
WhatsApp	«Настройки» → «Аккаунт» → «Двухэтапная проверка»	PIN-код из 6 цифр
Почта Gmail	«Управление аккаунтом Google» → «Безопасность» → «Двухэтапная аутентификация»	Код в приложении или SMS
Почта Mail.ru	«Настройки» → «Безопасность» → «Двухфакторная аутентификация»	Код в приложении или SMS
Банк, банк-клиент	Настройки безопасности в приложении банка	Код, биометрия, ЭЦП
eGov, Enbek.kz	Вход по ЭЦП	ЭЦП и пароль к ней

С чего начать

Рабочая почта — главный ключ: через нее восстанавливают пароли от всего остального. Если 2FA будет включена только в одном месте — пусть это будет почта.

16.4. ЭЦП: хранение и учет

- **Своя ЭЦП физического лица** — только для ваших личных действий: eGov, банк, сделки, суд. Для подписи от имени организации она не используется.
- **ЭЦП сотрудника организации** выпускается на работника для действий от имени работодателя (Enbek.kz, налоговая отчетность, электронный документооборот). Учитывается в журнале, при увольнении отзывается.
- **Носитель.**

  - **Ключ ЭЦП** — это файлы с расширением .p12. Откройте папку с ЭЦП и посмотрите на длинное обозначение ключа: GOST512_ДАЛЬШЕ ЦИФРЫ И БУКВЫ.p12. Чаще всего их хранят на флешке или в папке на компьютере: такой ключ можно скопировать, поэтому пароль к нему — единственная защита.
  - Надежнее — **токен**: специальный защищенный носитель, похожий на флешку (например, «Казтокен»), или удостоверение личности с чипом. Ключ записан внутри устройства, скопировать его нельзя, для подписи нужен ПИН-код. Вид носителя выбирают при выпуске ключа в НУЦ.
- **Хранение:** флешка с ключом или токен — в сейфе или запирающемся ящике; на компьютере — в папке, которой нет на рабочем столе. Пароль от ключа — не рядом с ключом и не на стикере.
- **Носитель** не оставлять в компьютере, уходя от стола и в конце дня. Хранить в сейфе или запирающемся ящике.
- **Передавать коллегам нельзя** — ни ключ, ни пароль. Нужна подпись в ваше отсутствие — выпускается ЭЦП сотрудника организации на другого работника или оформляется доверенность.
- **Раз в квартал** — проверка списка своих ключей в личном кабинете НУЦ РК. Неизвестный ключ — отозвать.

ЦИФРОВОЙ КАДРОВЫЙ АУДИТ
Проверьте свой кадровый учет и работу на сайте enbek.kz
https://www.hrdok.kz/esutd

16.5. Файлы с персональными данными работников

Задача	Как сделать безопасно
Отправить список работников с ИИН бухгалтеру или аутсорсеру	Заархивировать с паролем. 7-Zip: правой кнопкой по файлу → «7-Zip» → «Добавить к архиву…» → в разделе «Шифрование» ввести пароль, метод AES-256, отметить «Шифровать имена файлов». Пароль сообщить **другим каналом**: письмо — по почте, пароль — по телефону
Хранить личные дела в электронном виде	Сетевая папка или облако организации с доступом только кадровой службы. Не личный Google Диск, не облачные таблицы за рубежом
Получить данные удостоверения работника	Из личного дела в Enbek.kz, а не фото в мессенджер. Работник может проверить, что вы видите
Переписка с работником о его здоровье, семье, взысканиях	Рабочая почта или корпоративный мессенджер, а не личный WhatsApp

16.6. Увольнение работника или смена кадровика

Уволенный работник, у которого остались действующие доступы, — одна из самых частых причин утечки данных. Чаще всего это происходит не по злому умыслу: просто забыли. Учетная запись в 1С, рабочая почта, кабинет банк-клиента, рабочий чат, ключ ЭЦП сотрудника организации продолжают действовать неделями, а иногда и месяцами.

Работодатель обязан обеспечивать защиту персональных данных работников (пп. 24) п. 2 ст. 23 ТК РК), а несоблюдение мер по их защите влечет административную ответственность (ст. 79 КоАП РК). Поэтому отключение доступов — не техническая мелочь, а обязательная часть процедуры прекращения трудового договора.

Главное

Доступы отключает ответственный за кибербезопасность (ИТ-специалист). Кадровая служба запускает процесс: вовремя сообщает о дате прекращения трудового договора и контролирует, что все оформлено.

16.6.1. Кто что делает

Участник	Что делает
Кадровая служба	Сразу после издания акта о прекращении трудового договора направляет ответственному заявку на отключение доступов. Организует акт приема-передачи. Вносит сведения о прекращении в ЕСУТД не позднее 3 рабочих дней (п. 12 Правил ЕСУТД)
Непосредственный руководитель	Определяет, какие файлы, переписка и дела нужно передать и кому. Принимает дела у работника. Решает, кому переадресовать рабочую почту
Ответственный за кибербезопасность (ИТ)	Отключает учетные записи, меняет пароли общих учетных записей, принимает носители ключей ЭЦП, организует отзыв ЭЦП, проверяет журналы входов
Бухгалтерия	Отзывает доступ к банк-клиенту и платежным системам, если он был. Учитывает возврат техники
Работник	Передает дела, файлы, технику и носители ЭЦП. Подтверждает, что не хранит рабочие данные на личных устройствах

16.6.2. Порядок по срокам

Когда	Что сделать	Кто
В день издания акта о прекращении трудового договора	Заявка на отключение доступов с датой и временем отключения (образец ниже)	Кадровая служба

Когда	Что сделать	Кто
До последнего рабочего дня	Перечень доступов работника по акту ревизии учетных записей. Передача файлов и текущих дел. Решение о переадресации почты	Руководитель, ответственный
Последний рабочий день	Акт приема-передачи доступов и носителей ключей ЭЦП. Возврат техники. Отключение учетных записей по окончании рабочего дня	Ответственный, руководитель
Не позднее следующего рабочего дня	Отзыв ЭЦП сотрудника организации в НУЦ РК. Смена паролей общих учетных записей. Исключение из рабочих чатов. Отмена доверенностей, если они выдавались	Ответственный, руководитель организации
Не позднее 3 рабочих дней	Сведения о прекращении трудового договора в ЕСУТД	Кадровая служба
В течение месяца	Проверка журналов входов после даты увольнения. Отметка в акте ревизии учетных записей	Ответственный

Важно

Рабочую почту уволенного работника не удаляйте сразу. Переписка может понадобиться как доказательство в трудовом споре или проверке. Отключите вход, настройте переадресацию на руководителя и сохраните архив на срок, установленный работодателем.

16.6.3. Особые ситуации

Ситуация	Как действовать
Конфликтное увольнение, расторжение по инициативе работодателя, в том числе дисциплинарное	Доступы отключаются в момент вручения акта о прекращении трудового договора, а не в конце дня. Заявку ответственному направить заранее, время отключения согласовать. Копировать рабочие файлы после вручения работнику не разрешается
Дистанционный работник	Рабочие данные могли остаться на личном ноутбуке и в личном мессенджере. Получите письменное подтверждение работника об удалении рабочих данных с личных устройств (образец ниже). Техника работодателя возвращается по акту

Ситуация	Как действовать
Работник с доверенностью или правом подписи	Доверенность отменяется (ст. 170 ГК РК). Об отмене уведомите тех, перед кем работник представлял организацию: банк, контрагентов, государственные органы
Работник в отпуске или на больничном до даты увольнения	Доступы отключаются в дату прекращения трудового договора. Носители ЭЦП и технику передать в первый возможный день, отразить в акте
Работник был администратором рабочего чата или группы	До отключения передать права владельца или администратора другому работнику. Иначе управление чатом будет потеряно

16.6.4. Если уходит сам кадровик

Кадровик держит в руках больше всего доступов к персональным данным работников. Поэтому его увольнение или смена — отдельный сценарий, который нужно провести особенно тщательно.

1. **Кабинет работодателя на Enbek.kz.** Отозвать ЭЦП сотрудника организации, выпущенную на кадровика. Новому кадровику выпускается своя ЭЦП, а не передается старая.
2. **Доверенности.** Отменить доверенность на подписание кадровых документов, оформить новую на нового работника.
3. **Общие учетные записи.** Сменить пароли от общей почты отдела кадров, 1С, облачных папок с личными делами.
4. **Документы.** Передать по акту личные дела, журналы регистрации, трудовые договоры, листы ознакомления, электронные папки.
5. **Рабочие чаты с работниками.** Передать права администратора, удалить уходящего кадровика из чатов.
6. **Личный телефон.** Получить письменное подтверждение, что копии документов с персональными данными работников удалены из личного телефона и мессенджеров.

16.6.5. Чего делать нельзя

Нельзя	Почему
Требовать у работника пароли от его личных аккаунтов	Личные аккаунты работника не являются собственностью работодателя
Читать личную переписку работника в его мессенджерах	Это вмешательство в частную жизнь
Передавать новому работнику ЭЦП уволенного	Каждый работает под своей ЭЦП. Чужая ЭЦП — подпись за другого человека

Нельзя	**Почему**
Оставлять учетную запись «на всякий случай»	Если вы не отключили учетную запись уволенному работнику, то предоставили открытый доступ к данным компании
Удалять почту и файлы сразу после увольнения	Они могут понадобиться как доказательства

ПРИМЕРНЫЙ ОБРАЗЕЦ

ЗАЯВКА на отключение доступов

Ответственному за обеспечение кибербезопасности

Омарову Е. Н.

менеджера по персоналу Ермековой Ж. Б.

Сообщаю, что трудовой договор с Касымовым Ержаном Талгатовичем, кладовщиком, прекращается 23 октября 2026 года на основании приказа № 109-к от 16.10.2026.

Прошу:

1) отключить учетные записи работника во всех информационных системах ТОО 23.10.2026 по окончании рабочего дня, в 18:00;
2) принять носитель ключа ЭЦП сотрудника организации и организовать отзыв ЭЦП;
3) исключить работника из рабочих чатов ТОО;
4) рабочую почту sklad@dostar.kz переадресовать на заведующего складом Нурланова Д. Е.;
5) составить акт приема-передачи доступов в последний рабочий день.

Приложение: перечень учетных записей и доступов работника на 1 л.

_____ Ж. Б. Ермекова

16 октября 2026 года

ПРИМЕРНЫЙ ОБРАЗЕЦ

ПОДТВЕРЖДЕНИЕ РАБОТНИКА

Я, Касымов Ержан Талгатович, подтверждаю, что:

1) передал(а) работодателю все документы, файлы и материалы, полученные в связи с работой;
2) не храню на личных устройствах, в личной почте и мессенджерах документы, содержащие персональные данные работников и клиентов ТОО «Достар-KZ», а также иную информацию работодателя;
3) вернул(а) носитель ключа ЭЦП сотрудника организации и технику работодателя по акту приема-передачи.

_____ Е. Т. Касымов

ПРОЕКТ «КАБИНЕТ КАДРОВИКА» — вебинары и разборы весь год,
https://www.hrdok.kz/kabinet

Обратите внимание

Подтверждение подписывается добровольно. Если работник отказывается, составьте акт об отказе и зафиксируйте, что работнику было предложено передать и удалить рабочие данные. Это пригодится, если позднее данные окажутся у посторонних лиц.

16.6.6. Чек-лист увольнения

☐	Действие
☐	Заявка на отключение доступов направлена в день издания акта о прекращении
☐	Дела, файлы и рабочая переписка переданы руководителю или новому работнику
☐	Акт приема-передачи доступов и носителей ЭЦП составлен
☐	Техника работодателя возвращена
☐	Учетные записи отключены, пароли общих учетных записей изменены
☐	ЭЦП сотрудника организации отозвана, доверенности отменены
☐	Работник исключен из рабочих чатов, права администратора переданы
☐	Рабочая почта переадресована и сохранена
☐	Подтверждение об удалении рабочих данных получено или составлен акт об отказе
☐	Сведения о прекращении трудового договора внесены в ЕСУТД
☐	Отметка внесена в акт ревизии учетных записей

16.7. Если произошел инцидент

Время	Что сделать
Сразу	Не продолжать: закрыть окно, ничего не вводить. Отключить компьютер от сети, если открыли подозрительный файл
В течение 15 минут	Сообщить ответственному за кибербезопасность и непосредственному руководителю — устно и письменно (форма ниже)
В течение часа	Сменить пароли с другого, чистого устройства; завершить чужие сеансы; при утечке ЭЦП — отозвать ключ

Время	Что сделать
В течение дня	Ответственный вносит запись в журнал инцидентов, определяет, затронуты ли персональные данные работников, и докладывает руководителю
Деньги	Банк — по номеру телефона в приложении; полиция — 102

16.8. Антивирус: что делает и как с ним работать

Антивирус часто воспринимают как программу, которая «тормозит компьютер и не дает скачать нужный файл». Поэтому его отключают, ставят в исключения все подряд или годами не обновляют. На деле это последняя линия защиты, когда человек уже нажал не туда.

Что антивирус делает	Чего антивирус не делает
1) Проверяет файлы в момент скачивания и открытия: вложения, архивы, флешки. 2) Блокирует известные вредоносные программы: шпионов, шифровальщиков, программы удаленного управления. 3) Предупреждает о подозрительных сайтах и загрузках. 4) Защищает папки с документами от шифрования (функция защиты от программ-шантажистов).	• Не спасает, если вы сами ввели код или пароль на поддельной странице: это не вирус, а обман. • Не защищает от новой угрозы, если базы не обновлялись. • Не помогает, если отключен или файл добавлен в исключения. • Не заменяет внимательность: срочность и «никому не говорите» он не распознает.

Встроенный антивирус Windows уже есть

В Windows 10 и 11 встроен бесплатный антивирус — **Microsoft Defender** («Безопасность Windows»). Для домашнего и небольшого рабочего компьютера его достаточно, если он включен и обновляется. Если в компании установлен другой лицензионный антивирус, Defender отключается автоматически.

Задача	Где и как
Проверить, что защита включена	«Пуск» → «Параметры» → «Конфиденциальность и защита» (в Windows 10 — «Обновление и безопасность») → «Безопасность Windows» → «Защита от вирусов и угроз». Должна быть зеленая галочка и включена «Защита в режиме реального времени»

Задача	Где и как
Обновить базы вручную	Там же → «Обновления защиты от вирусов и угроз» → «Проверить наличие обновлений». Обычно базы обновляются сами каждый день, но после отпуска или долгого простоя компьютера — обновите вручную
Быстрая проверка	«Защита от вирусов и угроз» → «Быстрая проверка». Несколько минут
Полная проверка	«Параметры сканирования» → «Полное сканирование». Долго — запускайте в конце рабочего дня, раз в неделю или при подозрении
Если подозреваете серьезное заражение	«Параметры сканирования» → «Проверка автономным Microsoft Defender». Компьютер перезагрузится и проверится до запуска Windows
Защитить документы от шифровальщиков	«Защита от вирусов и угроз» → «Защита от программ-шантажистов» → «Контролируемый доступ к папкам» → включить. Незнакомые программы не смогут изменять файлы в папке «Документы»
Проверить один файл	Правой кнопкой по файлу → «Проверить с помощью Microsoft Defender»

Правила работы с антивирусом

Правило	Почему
Один антивирус на компьютере	Два антивируса мешают друг другу и замедляют работу, защита от этого не удваивается
Не отключать, даже «на минутку»	Именно в эту минуту открывают файл, который антивирус бы остановил
Не добавлять в исключения файлы и папки из интернета	Исключение — это разрешение не проверять
Обновлять базы и саму Windows	Антивирус узнает новые угрозы только из обновлений; обновления Windows закрывают уязвимости
Не устанавливать «взломанные» программы и «кряки»	Самый частый способ занести шпиона: антивирус на такой файл ругается, а человек его отключает

ПРОЕКТ «КАБИНЕТ КАДРОВИКА» — вебинары и разборы весь год,
https://www.hrdok.kz/kabinet

Правило	Почему
Предупреждение антивируса — не нажимать «Разрешить»	Закройте файл и сообщите ответственному за кибербезопасность. Если файл нужен для работы, решение принимает ответственный
Срок лицензии платного антивируса	Истекшая лицензия — антивирус без обновлений. Следите за сроком так же, как за сроком ЭЦП

Телефон

- **Android:** «Play Маркет» → значок профиля → «Play Защита» → включить проверку приложений. Устанавливать приложения только из «Play Маркета»; файлы .apk из мессенджеров не открывать.
- **iPhone:** отдельный антивирус не нужен — приложения ставятся только из App Store. Главное — вовремя устанавливать обновления iOS: «Настройки» → «Основные» → «Обновление ПО».

Для Требований по кибербезопасности

В акте работодателя достаточно трех строк:

1) на каждом рабочем компьютере установлен и включен антивирус с автоматическим обновлением баз;
2) работнику запрещено отключать его и добавлять исключения;
3) ответственный ежеквартально проверяет состояние защиты на всех компьютерах.

17. Кто отвечает за кибербезопасность: позиция кадровой службы

После изменений ТК РК многие руководители решили, что «кибербезопасность теперь в кадрах». Это не так. ТК РК возложил на работодателя две обязанности: ознакомить работников с требованиями и контролировать их исполнение (пп. 25-1) п. 2 ст. 23 ТК РК). Обеспечивать саму кибербезопасность закон обязывает собственника и владельца цифровых объектов, то есть организацию. Выполнять эту работу должны люди с профильной квалификацией.

17.1. Что такое кибербезопасность для бизнеса

> **§ Закон РК «О кибербезопасности», пп. 8) ст. 1**
> Кибербезопасность — **состояние защищенности цифровых объектов от нарушения их конфиденциальности, целостности или доступности**.

> **§ Цифровой кодекс РК, п. 2 ст. 20**
> К цифровым объектам относятся: 1) цифровые записи; 2) цифровые активы; 3) **цифровые ресурсы**; 4) **программное обеспечение**; 5) **цифровые системы**; 6) цифровые платформы; 7) **объекты цифровой инфраструктуры**; 8) продукты цифровых данных; 9) иные цифровые объекты…

Три слова из определения — это три вопроса, которые бизнес должен решить по каждому объекту: **конфиденциальность** — никто посторонний не видит данные; **целостность** — данные никто не изменил и не удалил; **доступность** — система работает, когда она нужна.

Цифровые объекты обычной компании	Примеры	Что требует защиты
Технические средства	Компьютеры, ноутбуки, рабочие и личные телефоны, принтеры, флешки	Пароли, шифрование дисков, обновления, учет и списание
Сеть	Роутер, Wi-Fi, сервер, сетевые папки, удаленный доступ	Настройка, разделение гостевой и рабочей сети, журналы подключений
Программы и учетные системы	1С: Бухгалтерия и ЗУП, Битрикс24, CRM, складские программы, банк-клиент	Права доступа, лицензии, обновления, резервные копии баз
Облачные сервисы	Google Workspace, облачные диски и таблицы, онлайн-сервисы ЭДО	Где физически хранятся данные, кто имеет доступ, 2FA
Почта, домен, сайт	Корпоративная почта, доменное имя, сайт, интернет-магазин, хостинг	Защита домена, резервные копии сайта, доступы администраторов

ПРОЕКТ «КАБИНЕТ КАДРОВИКА» — вебинары и разборы весь год,
https://www.hrdok.kz/kabinet

Цифровые объекты обычной компании	Примеры	Что требует защиты
Мессенджеры и соцсети	Рабочие чаты, аккаунты компании в Instagram, Telegram-канал	Администраторы, облачные пароли, правила переписки
ЭЦП и токены	ЭЦП организации, ЭЦП сотрудников организации, ЭЦП ИП	Хранение, выпуск и отзыв, журнал учета
Видеонаблюдение и СКУД	Камеры, пропускная система, биометрия	Хранение записей, доступ к архиву, обновление прошивок
Базы персональных данных	Работники, кандидаты, клиенты, покупатели	Перечень, меры защиты, ответственный, уведомление о нарушениях

Вывод

Из таблицы видно: кибербезопасность — это сети, серверы, программы, облака, домены, права доступа и резервное копирование. Это инженерная работа. Кадровая служба — один из пользователей этих систем, а не их администратор.

17.2. Карта: шесть уровней защиты

Карта кибербезопасности компании: шесть уровней защиты и кто выполняет работу на каждом

Уровень	Что входит	Кто выполняет
1. Сеть и периметр	Интернет-канал, роутер, межсетевой экран, Wi-Fi рабочий и гостевой, VPN и удаленный доступ, сегментация сети	**ИТ / ИБ** системный администратор, сетевой инженер
2. Серверы и хранилища	Сервер или сетевое хранилище, сетевые папки, права на каталоги, резервное копирование (бэкапы) и проверка восстановления, журналы событий	**ИТ / ИБ** системный администратор
3. Программы и базы	1С: Бухгалтерия и ЗУП, Битрикс24, CRM, банк-клиент, ЭДО: установка, обновления, учетные записи и роли, выгрузка копий баз	**ИТ + владелец процесса** ИТ настраивает; бухгалтер может делать выгрузку 1С по инструкции, если ему выданы права
4. Облака, почта, домен, сайт	Корпоративная почта и домен, DNS, хостинг и сайт, облачные диски и таблицы, 2FA и права администраторов	**ИТ / подрядчик** администратор почты и сайта, хостинг-провайдер
5. Устройства и ЭЦП	Компьютеры и телефоны: пароли, шифрование, антивирус, обновления; учет, выпуск и отзыв ключей ЭЦП, носители	**ИТ + ответственные** ИТ — настройка; работник — хранение своей ЭЦП; руководитель — решения о выпуске и отзыве
6. Люди и правила	Требования для работников, ознакомление под подпись, инструктаж при приеме, пятиминутки, сообщения об инцидентах, дисциплина	**Кадровая служба + все работники** кадры — ознакомление и документы; каждый работник — соблюдение

Примечание. Цвет столбца «Кто выполняет» показывает, чья это зона:

Только специалист с ИТ-квалификацией	**Совместно, по инструкции ИТ-специалиста**	**Зона кадровой службы**

Пять уровней из шести — сети, серверы, программы, облака и устройства — требуют технической квалификации.

Кадровая служба полностью отвечает только за шестой уровень — «люди и правила».

На третьем и пятом уровнях часть работы могут выполнять пользователи, но только по инструкции и с правами, которые выдал ИТ-специалист.

17.3. Кто обязан по закону

Обязанность	Кто обязан	Норма
Обеспечить кибербезопасность цифровых объектов	Собственник и владелец цифровых объектов — организация	пп. 1) п. 2 ст. 16, пп. 1) п. 2 ст. 17 Закона РК «О кибербезопасности»
Принимать правовые, организационные и технические меры защиты (средства защиты информации, системы контроля доступа и регистрации фактов доступа)	Собственник или владелец цифровых объектов	ст. 55 Закона РК «О кибербезопасности»
Принимать меры по защите персональных данных	Собственник и (или) оператор базы, содержащей персональные данные	ст. 25 Закона РК «О персональных данных и их защите»; ст. 56 Закона РК «О кибербезопасности»
Назначить лицо, ответственное за организацию обработки персональных данных	Собственник и (или) оператор — юридическое лицо	пп. 10) п. 2 ст. 25 Закона РК «О персональных данных и их защите»
Ознакомить работников с требованиями актов работодателя по кибербезопасности и контролировать исполнение	Работодатель	пп. 25-1) п. 2 ст. 23 ТК РК
Соблюдать требования кибербезопасности на рабочем месте	Каждый работник, включая кадровика	пп. 3) п. 2 ст. 22 ТК РК

Ни одна из этих норм не называет кадровую службу, бухгалтерию или юриста. Обязанность лежит на организации, а кто ее исполняет — решает руководитель, распределяя функции между работниками в соответствии с их трудовыми договорами.

17.4. Технические работы: почему нужна ИТ-квалификация

Работа	Простыми словами	Кто выполняет	Кадровик, бухгалтер
Настройка роутера, межсетевого экрана, Wi-Fi, VPN	Кто и откуда может подключиться к сети компании; гостевой Wi-Fi отделен от рабочего	Системный администратор, сетевой инженер	Нет
Сервер, сетевые хранилища, права на папки	Кто видит папку «Кадры» или «Бухгалтерия», кто может удалить файлы	Системный администратор	Нет. Кадровик сообщает, кому доступ нужен
Резервное копирование и проверка восстановления	Копия данных на случай шифровальщика, поломки или ошибки — и проверка, что из нее действительно можно все вернуть	Системный администратор	Нет
Резервная копия базы 1С	Выгрузка информационной базы	ИТ настраивает автоматическое копирование	Частично: бухгалтер может делать выгрузку по инструкции, если ему выданы права
Домен, DNS, корпоративная почта	Адреса @компания.kz, защита от писем-подделок от имени компании, продление домена	Администратор почты, подрядчик	Нет
Антивирус и обновления на всех компьютерах	Централизованная установка, контроль, что защита везде включена	Системный администратор	Нет. Работник только не отключает
Журналы событий, расследование инцидента	Кто, когда и откуда входил, что было изменено	Специалист по информационной безопасности	Нет. Кадровик принимает сообщение работника

Работа	Простыми словами	Кто выполняет	Кадровик, бухгалтер
Учетные записи при приеме и увольнении	Создать и отключить доступы в день приема и увольнения	ИТ — по заявке	Частично: заявка, сроки, акт приема-передачи
Требования для работников, ознакомление, инструктаж	Правила поведения и подтверждение, что работник их знает	Кадровая служба совместно с ответственным	Да

> **Важно**
> **Права администратора сети, сервера или почты у пользователя, который не владеет ими профессионально, — сами по себе угроза.** Одна ошибка в настройке открывает данные всей компании. Поэтому передать такие права кадровику «на всякий случай» — не решение, а новый риск.

17.5. Кто должен выполнять: профиль специалиста

Вариант	Когда подходит	Как оформить
Штатный системный администратор	Компания от 20–30 компьютеров, свой сервер, 1С на сервере	Трудовой договор, должностная инструкция с обязанностями по кибербезопасности
ИТ-аутсорсинг (приходящий администратор, обслуживающая компания)	Малый бизнес: несколько компьютеров, облачная 1С, почта у провайдера	Договор оказания услуг с перечнем работ, сроками реагирования и ответственностью
Специалист по информационной безопасности	Крупная компания, много систем, персональные данные клиентов в больших объемах	Трудовой договор; может быть отдельное подразделение
Центр обеспечения кибербезопасности	Владельцы критически важных цифровых объектов	В порядке, установленном Законом РК «О кибербезопасности»

Требование	Рекомендуемый уровень
Образование	Высшее или техническое и профессиональное по направлениям «Информационные технологии», «Информационная безопасность», «Вычислительная техника и программное обеспечение», «Системы связи»
Опыт работы	Системный администратор — от 1–2 лет администрирования; специалист по информационной безопасности — от 2–3 лет в ИТ или ИБ
Знания	Операционные системы Windows и (или) Linux; локальные сети, Wi-Fi, VPN; учетные записи и права доступа; резервное копирование и восстановление; антивирусы и межсетевые экраны; администрирование 1С; законодательство РК о персональных данных и кибербезопасности
Подтверждение	Диплом, сертификаты курсов по администрированию сетей, систем и информационной безопасности

Закон не устанавливает квалификационных требований к такому специалисту в обычной компании — это ориентир для руководителя при подборе. Для владельцев критически важных цифровых объектов требования строже.

Функционал ответственного за кибербезопасность

- Ведет перечень цифровых объектов компании и учет доступов к ним.
- Настраивает и обслуживает сеть, сервер, рабочие места, антивирусы, обновления.
- Организует резервное копирование и регулярно проверяет восстановление.
- Выдает и отзывает доступы по заявкам, ведет журнал учета ключей ЭЦП.
- Разрабатывает Требования по кибербезопасности для работников совместно с кадровой службой.
- Принимает сообщения об инцидентах, расследует их и докладывает руководителю.
- Ежеквартально проверяет состояние защиты и дает руководителю справку.

17.6. Административные штрафы

Нарушение	Норма КоАП РК	Должностные лица / малый бизнес, НКО	Средний бизнес	Крупный бизнес
Незаконные сбор и (или) обработка персональных данных	ч. 1 ст. 79	60 МРП	100 МРП	200 МРП
То же с использованием служебного положения	ч. 2 ст. 79	200 МРП	300 МРП	600 МРП

Нарушение	Норма КоАП РК	Должностные лица / малый бизнес, НКО	Средний бизнес	Крупный бизнес
Несоблюдение мер по защите персональных данных	ч. 3 ст. 79	300 МРП	450 МРП	600 МРП
То же, повлекшее утерю, незаконный сбор и (или) обработку персональных данных	ч. 4 ст. 79	750 МРП	1 000 МРП	2 000 МРП
Неосуществление или ненадлежащее осуществление мер защиты цифровых систем и баз, содержащих персональные данные; нарушение единых требований в сферах цифровизации и кибербезопасности	ч. 1 ст. 641	75 МРП	300 МРП	1 000 МРП
Использование цифровых ресурсов с персональными данными во вред лицам	ч. 4 ст. 641	20 МРП	40 МРП	200 МРП

Для физических лиц предусмотрены отдельные размеры штрафов: например, по ч. 3 ст. 79 — 150 МРП, по ч. 4 ст. 79 — 200 МРП. КоАП РК по состоянию на 20.08.2026.

17.7. Что делает кадровая служба, а что — нет

Зона кадровой службы	Не зона кадровой службы
1) Участвовать в подготовке акта работодателя в части трудовых отношений: ознакомление, дисциплина, обязанности работников. 2) Знакомить работников с требованиями под подпись и хранить листы ознакомления. 3) Включать требования в трудовые договоры, должностные инструкции, правила трудового распорядка. 4) Защищать персональные данные работников в кадровых документах и личных делах. 5) Сообщать ответственному о нарушениях и инцидентах, оформлять дисциплинарные взыскания по представлению ответственного.	• Выбирать, устанавливать и настраивать средства защиты, антивирусы, сети, серверы. • Администрировать 1С, Битрикс24, CRM, почту, домены, облака. • Выдавать и отзывать технические доступы, вести журналы событий. • Делать резервные копии и восстанавливать данные. • Расследовать технические инциденты и оценивать уязвимости.

ОБУЧЕНИЕ И ПОВЫШЕНИЕ КВАЛИФИКАЦИИ:

самостоятельно планируете и проводите внутренний кадровый аудит, оцениваете уровень риска, составляете итоговый аудиторский отчет и проводите восстановление учета

— «Риск-ориентированный кадровый аудит»

https://www.hrdok.kz/audit

ПРИМЕРНЫЙ ОБРАЗЕЦ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Директору ТОО «Достар-KZ»
Нурмагамбетову А. С.
менеджера по персоналу Ермековой Ж. Б.

О распределении обязанностей по обеспечению кибербезопасности

В связи с устным поручением от 03.11.2026 «взять на себя кибербезопасность» сообщаю следующее.

1. **Кто обязан обеспечивать кибербезопасность.** Кибербезопасность — состояние защищенности цифровых объектов от нарушения их конфиденциальности, целостности или доступности (пп. 8) ст. 1 Закона РК «О кибербезопасности»).

Обязанность обеспечить кибербезопасность цифровых объектов возложена на их собственника и владельца, то есть на ТОО (пп. 1) п. 2 ст. 16, пп. 1) п. 2 ст. 17 Закона). Цифровыми объектами ТОО являются: компьютеры и телефоны работников, локальная сеть и Wi-Fi, 1С: Бухгалтерия и ЗУП, Битрикс24, банк-клиент, корпоративная почта и домен dostar.kz, сайт, облачные диски, рабочие мессенджеры, ЭЦП организации и сотрудников, система видеонаблюдения, базы персональных данных работников и клиентов.

2. **Что требует закон.** Защита цифровых объектов включает правовые, организационные и технические меры, в том числе использование средств защиты информации, систем контроля доступа и регистрации фактов доступа (ст. 55 Закона). ТОО как собственник базы персональных данных обязано принимать меры по их защите и назначить лицо, ответственное за организацию обработки персональных данных (ст. 25 Закона РК «О персональных данных и их защите»). Трудовой кодекс дополнительно обязывает работодателя ознакомить работников с требованиями актов работодателя по кибербезопасности и контролировать их исполнение (пп. 25-1) п. 2 ст. 23 ТК РК).
3. **Риски ТОО.** За несоблюдение мер по защите персональных данных предусмотрен штраф на субъектов малого предпринимательства 300 МРП, а при утере или незаконной обработке данных — 750 МРП (ч. 3, 4 ст. 79 КоАП РК); за неосуществление мер защиты цифровых систем, содержащих персональные данные, — 75 МРП (ч. 1 ст. 641 КоАП РК). Штрафы предусмотрены и для должностных лиц.
4. **Объем работ требует технической квалификации.** Обеспечение кибербезопасности ТОО включает: настройку и контроль локальной сети, Wi-Fi и удаленного доступа; управление сервером, сетевыми хранилищами и правами доступа к папкам; резервное копирование баз 1С, почты и сайта и проверку восстановления; администрирование домена dostar.kz и корпоративной почты; централизованную установку и обновление антивирусов; анализ журналов событий и реагирование на инциденты. Эти работы требуют образования и опыта в сфере информационных технологий или информационной безопасности, а также прав администратора информационных систем. Передача таких прав работнику, который не владеет ими профессионально, сама по себе создает угрозу для данных ТОО. Кадровая служба не обладает такой квалификацией. Моя трудовая функция определена трудовым договором от 01.06.2026 и должностной инструкцией менеджера по персоналу; поручение работы по другой специальности и квалификации допускается только с согласия работника (пп. 4) п. 2 ст. 23, ст. 38 ТК РК).
5. **Предлагаю:**

1) назначить ответственным за обеспечение кибербезопасности специалиста с образованием и опытом в сфере информационных технологий — штатного системного администратора или ИТ-компанию по договору оказания услуг с перечнем работ;

2) назначить лицо, ответственное за организацию обработки персональных данных (пп. 10) п. 2 ст. 25 Закона РК «О персональных данных и их защите»), из числа руководителей или юристов ТОО;

3) поручить ответственному провести ревизию цифровых объектов и доступов и подготовить Требования по кибербезопасности;

4) возложить на кадровую службу ознакомление работников с Требованиями, включение их в трудовые договоры и должностные инструкции, хранение листов ознакомления — эти функции входят в мои обязанности, и я готова их выполнить.

Приложения: перечень цифровых объектов ТОО на 1 л.; карта распределения работ по кибербезопасности на 1 л.

_____ Ж. Б. Ермекова

5 ноября 2026 года

Зарегистрировано в журнале регистрации внутренних документов № 113 от 05.11.2026

Как пользоваться

Записка — это не саботаж и не отказ от работы, а предложение распределить новые обязанности законно:

1) с учетом доступов,
2) полномочий и квалификации штатных и привлеченных специалистов.
3) Каждое утверждение в ней опирается на норму, поэтому руководителю сложно отмахнуться от нее как от «нежелания работать».

Аргументы из этого раздела подходят и для письменного, и для устного разговора с руководителем: о том, что такое кибербезопасность на самом деле, кто обязан ее обеспечивать по закону и какие работы в ней требуют технической квалификации.

Записку составьте в двух экземплярах. Первый передайте руководителю с регистрацией в журнале внутренних документов, второй — с отметкой о регистрации — храните у себя.

АКАДЕМИЯ ТРУДОВОГО ПРАВА И КАДРОВЫХ КОМПЕТЕНЦИЙ HR UP SKILL

КУРС «Специалист отдела кадров»

Для тех, кто осваивает профессию, приходит в кадры из смежной сферы или хочет заново выстроить кадровый учет последовательно и системно.

Как проходит: каждую неделю — 3 живых вебинара в Zoom с разбором ваших вопросов, видеоуроки по каждой теме, практические задания, тренажеры и симуляции кадровых ситуаций, итоговые тестирования по темам, аттестация.

Что остается у вас: шаблоны документов, пошаговые алгоритмы и чек-листы, конспекты, записи всех занятий в личном кабинете на 12 месяцев.

Результат: уверенно оформляете прием, перевод, отпуск, увольнение, ведете ЕСУТД — и обосновываете каждый документ нормой ТК РК.

ttps://www.hrdok.kz/ok2026

КУРС «Управление трудовыми отношениями»

Для действующих кадровиков, HR, юристов и руководителей кадровых служб, которые хотят систематизировать практику и уверенно работать со сложными вопросами.

Как проходит: каждую неделю — 3 живых вебинара в Zoom, видеоуроки, разборы сложных случаев и судебной практики, внутренний аудит своей практики по контрольным листам по каждой теме.

ПРОЕКТ «КАБИНЕТ КАДРОВИКА» — вебинары и разборы весь год,
https://www.hrdok.kz/kabinet

Что остается у вас: контрольные листы внутреннего аудита, шаблоны, алгоритмы, конспекты, собственная карта кадровых рисков, записи занятий на 12 месяцев.

Результат: находите и закрываете пробелы в своей работе и аргументируете решения нормой и судебной практикой — перед руководителем, инспектором и в споре.

https://www.hrdok.kz/pravo-hr

КОНСУЛЬТАЦИОННЫЙ ПРОЕКТ «Кабинет кадровика»

Для тех, кто уже в профессии и не хочет оставаться один на один с изменениями законодательства и сложными ситуациями.

Результат: вовремя узнаете об изменениях ТК РК, разбираете реальные кейсы и всегда знаете, где спросить и на что опереться.

Внутри: вебинары каждую среду и их записи, конспекты с образцами, архив разборов, ответы на ваши вопросы в чате, Энциклопедия кадровых решений. Доступ на 12 месяцев, вебинары каждую среду, материалы для ежедневной кадровой работы в личном кабинете.

https://www.hrdok.kz/kabinet

Цифровой кадровый аудит: ЕСУТД и Enbek.kz

Самопроверка сведений в ЕСУТД, ответы со ссылками на нормы, образцы документов и судебная практика. Доступ сразу после оплаты.

Цифровое решение работает в браузере на казахстанском сервере.

https://www.hrdok.kz/esutd

Оплата от ИП или юрлица. Рассрочки Kaspi и Halyk банка
Подобрать программу —www.hrdok.kz

18. Пакет документов работодателя

Напоминание: отдельный акт о кибербезопасности закон не требует (письмо МТСЗН РК от 17.09.2026 № ЖТ-2026-03677189).

Требования можно включить в действующие акты. Ниже полный пакет для тех, кто решил оформить их отдельно. Порядок согласования и утверждения может быть аналогичным, а может отличаться: служебная записка → приказ → ревизия → требования → ознакомление → контроль.

№	Документ	Кто готовит	Кто подписывает
1	Служебная записка о необходимости мер	Кадровая служба	Менеджер по персоналу
2	Приказ о мерах по обеспечению кибербезопасности	Кадровая служба совместно с ИТ	Директор

№	Документ	Кто готовит	Кто подписывает
3	Акт ревизии учетных записей и доступов	Ответственный за кибербезопасность	Комиссия
4	Требования по кибербезопасности для работников	Ответственный (ИТ) при участии кадровой службы	Утверждает директор
5	Журнал учета ключей ЭЦП	Ответственный	—
6	Лист ознакомления	Кадровая служба	Работники
7	Сообщение об инциденте и журнал инцидентов	Работник / ответственный	—
8	Акт приема-передачи доступов при увольнении	Ответственный	Передающий и принимающий

ПРИМЕРНЫЙ ОБРАЗЕЦ

СЛУЖЕБНАЯ ЗАПИСКА

Директору ТОО «Достар-KZ»
Нурмагамбетову А. С.
от менеджера по персоналу Ермековой Ж. Б.

О мерах по обеспечению кибербезопасности

С 25 августа 2026 года работник обязан соблюдать требования кибербезопасности на рабочем месте (пп. 3) п. 2 ст. 22 ТК РК), а работодатель — ознакомить работников с требованиями актов работодателя по кибербезопасности и осуществлять внутренний контроль за их исполнением (пп. 25-1) п. 2 ст. 23 ТК РК). Работодатель также обязан обеспечивать защиту персональных данных работников (пп. 24) п. 2 ст. 23 ТК РК).

29–30 октября 2026 года в профессиональных Telegram-группах прошла фишинговая рассылка, в результате которой были захвачены аккаунты участников. В ТОО работники используют личные мессенджеры для рабочей переписки, ЭЦП сотрудников организации хранятся у пользователей, учет учетных записей и ключей не ведется.

В связи с изложенным предлагаю:

1) назначить ответственного за обеспечение кибербезопасности (штатного работника или привлеченного ИТ-специалиста по договору);
2) создать комиссию и провести до 30.11.2026 ревизию учетных записей, ключей ЭЦП и доступов работников к информационным системам ТОО;
3) по результатам ревизии утвердить Требования по кибербезопасности для работников ТОО, включая порядок сообщения об инцидентах;
4) поручить кадровой службе организовать ознакомление работников с утвержденными Требованиями и хранение листов ознакомления.

Разработка технических мер защиты, настройка информационных систем и контроль их исполнения требуют специальных знаний и не входят в мои должностные обязанности. Со своей стороны обеспечу подготовку проекта приказа, ознакомление работников и учет документов.

Приложение: проект приказа на 2 л.

_____ Ж. Б. Ермекова

5 ноября 2026 года

Зарегистрировано в журнале регистрации внутренних документов № 112 от 05.11.2026

> **Как использовать**
>
> Записку составьте в двух экземплярах: один передается руководителю с регистрацией в журнале внутренних документов, второй с отметкой о регистрации остается у вас. Это доказательство, что кадровая служба вопрос подняла и решение предложила.

ПРИМЕРНЫЙ ОБРАЗЕЦ

«О мерах по обеспечению кибербезопасности»

В соответствии с пп. 24), 25-1) п. 2 ст. 23 Трудового кодекса Республики Казахстан **ПРИКАЗЫВАЮ:**

1) Назначить ответственным за обеспечение кибербезопасности в ТОО «Достар-KZ» **Омарова Ерлана Нурлановича**, ИТ-специалиста (договор оказания услуг № 21 от 01.03.2026).
2) Создать комиссию по ревизии учетных записей и доступов в составе: председатель — Омаров Е. Н.; члены — Сейтенова А. Б., главный бухгалтер; Ермекова Ж. Б., менеджер по персоналу.
3) Комиссии в срок до 30.11.2026 провести ревизию учетных записей, ключей ЭЦП и доступов работников к информационным системам ТОО и составить акт.
4) Омарову Е. Н. в срок до 10.12.2026 с учетом результатов ревизии подготовить проект Требований по кибербезопасности для работников ТОО.
5) Ермековой Ж. Б. в течение 5 рабочих дней после утверждения Требований ознакомить с ними работников под подпись, с вновь принимаемыми — при приеме на работу до начала работы.
6) Контроль за исполнением приказа оставляю за собой.

Директор _____ А. С. Нурмагамбетов

С приказом ознакомлены:

> **Обратите внимание**
>
> Если ответственный — привлеченный специалист по договору оказания услуг, он не работник: приказ для него не обязателен. Его обязанности по ревизии и подготовке Требований пропишите в договоре, а в приказе укажите ссылку на договор.

Акт ревизии учетных записей и доступов (форма)

Ревизия — это инвентаризация доступов. В акт вносятся не пароли, а учетные записи и сведения о защите.

ТОО «Достар-KZ»

г. Алматы

АКТ № 1

О проведении ревизии учетных записей и доступов работников к информационным системам

Основание: приказ директора ТОО «Достар-KZ» № 45-п от 12.11.2026 «О мерах по обеспечению кибербезопасности».

Комиссия: председатель Омаров Е. Н., ИТ-специалист (ответственный за обеспечение кибербезопасности); члены комиссии: Сейтенова А. Б., главный бухгалтер; Ермекова Ж. Б., менеджер по персоналу.

Период проверки: с 16.11.2026 по 27.11.2026.

Что проверялось: наличие у работников учетных записей в информационных системах ТОО, способ входа, включение двухфакторной аутентификации, хранение ключей ЭЦП, отключение доступов уволенных работников.

Сокращения и термины

Термин	Что означает
Учетная запись	Логин, под которым работник входит в систему (почта, Enbek.kz, банк-клиент, 1С, мессенджер)
2FA (двухфакторная аутентификация)	Вход по двум признакам: пароль и второй признак, которого нет у постороннего (код из SMS или приложения, ключ ЭЦП, облачный пароль). Без второго признака украденный пароль не дает войти
ЭЦП сотрудника организации	Ключ электронной цифровой подписи, выпущенный на работника для действий от имени ТОО
Нарушений не выявлено	Учетная запись используется по назначению, вход защищен, доступ соответствует должностным обязанностям

Результаты проверки

№	Работник, система, учетная запись	Защита входа	Результат проверки	Мера, срок, кто отвечает
1	Ермекова Ж. Б., менеджер по персоналу Enbek.kz (ЕСУТД), кабинет работодателя ТОО	ЭЦП сотрудника организации (флешка № 1) и пароль к ключу. 2FA: да	**Нарушений не выявлено**	Не требуется

№	Работник, система, учетная запись	Защита входа	Результат проверки	Мера, срок, кто отвечает
2	Ермекова Ж. Б., менеджер по персоналу Корпоративная почта hr@dostar.kz	Пароль. 2FA: нет	**2FA не включена**	Включить двухфакторную аутентификацию Срок: до 05.12.2026 Отвечает: Омаров Е. Н.
3	Сейтенова А. Б., главный бухгалтер Банк-клиент, логин buh_dostar	ЭЦП и код из SMS. 2FA: да	**Нарушений не выявлено**	Не требуется
4	Касымов Е. Т., кладовщик, трудовой договор прекращен 23.10.2026 1С: Зарплата и управление персоналом, логин kasymov	Пароль. 2FA: нет	**Учетная запись уволенного работника не отключена**	Отключить учетную запись, проверить журнал входов после 23.10.2026 Срок: немедленно, 28.11.2026 Отвечает: Омаров Е. Н.
5	Все работники (14 человек) Рабочий Telegram-чат ТОО, личные аккаунты работников	Код из SMS. Облачный пароль у 6 из 14	**У 8 работников облачный пароль не установлен**	Провести инструктаж, проверить установку облачного пароля у каждого Срок: до 10.12.2026 Отвечает: Ермекова Ж. Б.

Итоги

Проверено учетных записей: 5 групп, 14 работников.

Выявлено нарушений: 3, в том числе 1 требует немедленного устранения (позиция 4).

Предложения комиссии: включить в Требования по кибербезопасности обязательную двухфакторную аутентификацию для корпоративной почты; установить порядок отключения учетных записей в день прекращения трудового договора по заявке кадровой службы; провести повторную проверку до 25.12.2026.

Председатель комиссии _____ Е. Н. Омаров

Члены комиссии _____ А. Б. Сейтенова

_____ Ж. Б. Ермекова

С актом ознакомлен:

Директор ТОО «Достар-KZ» _____ А. С. Нурмагамбетов

«___» _____ 2026 г.

ОБРАЗЕЦ

УТВЕРЖДЕНЫ
приказом директора ТОО «Достар-KZ»
от 10 декабря 2026 года № 51-п

ТРЕБОВАНИЯ
по кибербезопасности для работников ТОО «Достар-KZ»

1. Общие положения

1.1. Настоящие Требования разработаны в соответствии с подпунктом 3) пункта 2 статьи 22, подпунктами 24), 25-1) пункта 2 статьи 23 Трудового кодекса Республики Казахстан и законодательством Республики Казахстан о персональных данных и их защите.

1.2. Требования обязательны для всех работников ТОО «Достар-KZ» (далее — ТОО) независимо от должности и формы работы, в том числе дистанционной.

1.3. Работник знакомится с Требованиями под подпись при приеме на работу до начала работы, а также при каждом изменении Требований.

1.4. Ответственным за обеспечение кибербезопасности в ТОО является лицо, назначенное приказом директора (далее — ответственный).

2. Учетные записи и пароли

2.1. Каждый работник работает только под своей учетной записью. Использование чужой учетной записи запрещено.

2.2. Пароль должен:

1) состоять не менее чем из 12 символов;
2) быть уникальным для каждой информационной системы;
3) меняться при подозрении на компрометацию и при передаче дел.

2.3. Запрещается:

1) записывать пароли на стикерах и хранить их в незашифрованных файлах;
2) сообщать пароли другим лицам, в том числе по телефону и в мессенджерах;
3) сохранять пароли в браузере на компьютере общего пользования.

2.4. В корпоративной почте и мессенджерах, используемых для работы, включается двухфакторная аутентификация.

3. Рабочее место

3.1. Покидая рабочее место, работник блокирует экран (сочетание клавиш Win + L).

3.2. Автоматическая блокировка экрана устанавливается не более чем через 5 минут бездействия.

3.3. На рабочем компьютере должен быть включен антивирус с автоматическим обновлением баз.

3.4. Запрещается:

1) отключать антивирус;
2) добавлять файлы и папки в исключения антивируса без согласования с ответственным;
3) устанавливать нелицензионные программы;
4) откладывать обновления операционной системы более чем на 3 дня.

4. Электронная цифровая подпись

4.1. Учет ключей ЭЦП сотрудников организации ведет ответственный в журнале учета ключей ЭЦП.

4.2. Передача ключа ЭЦП и пароля к нему другому лицу запрещена.

4.3. Носитель ключа ЭЦП извлекается из компьютера после использования и хранится в запирающемся ящике или сейфе.

4.4. О потере носителя или компрометации пароля работник сообщает ответственному незамедлительно.

5. Электронная почта, мессенджеры, ссылки и файлы

5.1. Документы с персональными данными работников передаются только через корпоративную почту, архивом с паролем. Пароль к архиву сообщается другим каналом связи.

5.2. Запрещается открывать файлы с расширениями .exe, .apk, .scr, .bat и архивы с паролем, полученные от неизвестных отправителей.

5.3. Коды подтверждения из SMS, Telegram, 1414, eGov никому не сообщаются.

5.4. Распоряжение об оплате по новым реквизитам исполняется только после подтверждения звонком по известному номеру в порядке, установленном Порядком согласования и проведения платежей.

6. Инциденты

6.1. Работник обязан сообщить ответственному и непосредственному руководителю о подозрительном сообщении, переходе по ссылке, вводе кода, потере носителя ЭЦП:

1) устно — незамедлительно;
2) письменно — не позднее 15 минут с момента инцидента.

6.2. Работник, своевременно сообщивший об инциденте, за сам факт перехода по ссылке к дисциплинарной ответственности не привлекается.

7. Внутренний контроль

7.1. Ответственный не реже одного раза в квартал проверяет:

1) актуальность учетных записей работников;
2) включение двухфакторной аутентификации;
3) отзыв ключей ЭЦП и отключение доступов уволенных работников.

7.2. Не реже двух раз в год ответственный проводит учебные проверки (учебные фишинговые сообщения). Результаты обсуждаются без указания имен и основанием для дисциплинарного взыскания не являются.

7.3. Результаты контроля оформляются справкой на имя директора.

8. Ответственность

8.1. Неисполнение Требований работником, ознакомленным с ними под подпись, является нарушением трудовой дисциплины и может повлечь дисциплинарное взыскание в порядке, установленном статьями 64–66 Трудового кодекса Республики Казахстан.

Конец образца

Почему так сформулировано

Пункт 6.2 — не «послабление», а инструмент: если за сообщение об ошибке наказывают, о ней молчат, и ущерб растет.

Дисциплинарную ответственность можно применить только за нарушение требований, с которыми работник ознакомлен под подпись. Поэтому лист ознакомления — главный документ всего пакета.

Журнал учета ключей ЭЦП сотрудников организации (форма)

№	Работник, должность	Ключ и носитель	Срок действия	Где хранится	Отзыв
1	Ермекова Ж. Б., менеджер по персоналу	Сотрудник организации (кадры, Enbek.kz), флешка № 1	до 14.03.2027	Сейф кадровой службы	—
2	Сейтенова А. Б., главный бухгалтер	Сотрудник организации с правом подписи, токен (Казтокен) № 2	до 02.06.2027	Сейф бухгалтерии	—
3	Касымов Е. Т., кладовщик	Сотрудник организации, файл на ПК склада	до 10.01.2027	ПК склада	Отозван 24.10.2026

ПРИМЕРНЫЙ ОБРАЗЕЦ

ЛИСТ ОЗНАКОМЛЕНИЯ

с Требованиями по кибербезопасности для работников ТОО «Достар-KZ», утвержденными приказом № 51-п от 10.12.2026

Подписывая, подтверждаю, что Требования мне разъяснены, экземпляр доступен мне в сетевой папке «Акты работодателя», обязуюсь их соблюдать (пп. 3) п. 2 ст. 22 ТК РК).

1. Ермекова Жанна Болатовна, менеджер по персоналу _____ 11.12.2026
2. Сейтенова Асель Бекетовна, главный бухгалтер _____ 11.12.2026
3. Нурланов Данияр Ерланович, водитель _____ 12.12.2026

Электронно

Ознакомление можно провести электронно — через систему электронного документооборота с ЭЦП работника. Тогда лист ознакомления формируется в системе.

ПРИМЕРНЫЙ ОБРАЗЕЦ

СООБЩЕНИЕ ОБ ИНЦИДЕНТЕ

Кому: ответственному за кибербезопасность Омарову Е. Н.; копия — главному бухгалтеру Сейтовой А. Б.

Дата и время: 15.12.2026, 10:42

Что произошло: в рабочем Telegram-чате от аккаунта коллеги пришло сообщение «Чат переносится в новую группу». Я перешла по ссылке, открылось окно бота, ввела код, который пришел в Telegram.

Что уже сделано: в 10:47 завершила все другие сеансы, включила облачный пароль, предупредила рабочий чат.

Затронутые данные: в переписке есть файл со списком работников и ИИН от 02.12.2026.

_____ Ж. Б. Ермекова

Дата, время, работник	Что произошло	Затронуты ли ПДн	Принятые меры, ответственный
15.12.2026, 10:42 Ермекова Ж. Б.	Ввод кода в фишинговом боте Telegram	Да: список работников с ИИН	Сеансы завершены, облачный пароль, предупреждение чата, оценка утечки Омаров Е. Н.

Журнал инцидентов (фрагмент). При затрагивании персональных данных ответственный оценивает последствия и действия по законодательству о персональных данных и их защите.

ПРИМЕРНЫЙ ОБРАЗЕЦ

АКТ ПРИЕМА-ПЕРЕДАЧИ ДОСТУПОВ

г. Алматы 23 октября 2026 года

Касымов Ержан Талгатович, кладовщик (передает), и Омаров Ерлан Нурланович, ответственный за кибербезопасность (принимает), составили акт о следующем:

1. Передан носитель ЭЦП сотрудника организации — флешка № 3. Ключ отозван 24.10.2026.

2. Учетная запись «kasymov» в 1С: Зарплата и кадры — отключена 23.10.2026, 17:10.

3. Рабочая почта sklad@dostar.kz — пароль изменен, доступ передан Нурланову Д. Е.

4. Исключен из рабочих чатов: «Склад», «Достар — общий» — 23.10.2026.

5. Личные устройства работника рабочих данных не содержат — со слов работника.

Передал _____ Е. Т. Касымов Принял _____ Е. Н. Омаров

19. Мы это уже разбирали в «Кабинете кадровика»

Вебинар	Дата	Тема
№ 8	4 марта	Работа на Enbek.kz: ЭЦП и доступ к ЕСУТД, доверенность, смена кадровика
№ 16	20 мая	Изменения ТК и правил ЕСУТД: пуш-коды и ЭЦП — что не равно подписи
№ 19	17 июня	Изменения ТК: частная жизнь работника, контактные данные, фото и видео
№ 25	30 июля	Проверка ГИТ: копии вместо подлинников, защита персональных данных
№ 28	12 августа	Кибербезопасность в ТК: положение, памятка по кибергигиене, правило одной ЭЦП
№ 29	19 августа	Персональные данные работников, часть 1: утечки, согласие, фото
№ 30	26 августа	Персональные данные, часть 2: инцидент, акт о кибербезопасности, ответственность
№ 32	9 сентября	Персональные данные и кибербезопасность: что реально касается кадровика
№ 33	16 сентября	Паника в соцсетях и границы ответственности кадровика
№ 36	7 октября	Отказ подписать согласие на обработку данных, электронное ознакомление

ОБУЧЕНИЕ И ПОВЫШЕНИЕ КВАЛИФИКАЦИИ:

не оставайтесь один на один со сложными ситуациями и изменениями законодательства. «КАБИНЕТ КАДРОВИКА» — профессиональное сопровождение кадровика весь год

https://www.hrdok.kz/kabinet

20. Официальные адреса и чек-лист «Проверьте себя за 15 минут»

Сервис	Официальный адрес или номер
Электронное правительство	egov.kz, приложение eGov Mobile
Национальный удостоверяющий центр (ЭЦП)	pki.gov.kz
Enbek.kz (ЕСУТД)	enbek.kz
Комитет государственных доходов	kgd.gov.kz, контакт-центр 1414
Первое кредитное бюро	1cb.kz
Поддержка Telegram	telegram.org/support
Полиция	102
Банк	Номер на обратной стороне вашей карты или в официальном приложении

☐	Действие	Время
☐	Облачный пароль в Telegram включен, записан и хранится дома	3 мин
☐	В «Устройствах» Telegram и «Связанных устройствах» WhatsApp нет чужих входов	2 мин
☐	Двухэтапная проверка в WhatsApp включена	2 мин
☐	2FA в рабочей и личной почте включена	3 мин
☐	Номер телефона скрыт, звонки и приглашения — только от контактов	2 мин
☐	На компьютере стоит пароль, автоблокировка 5 минут, я знаю Win + L	1 мин
☐	В Проводнике включен показ расширений файлов	1 мин
☐	Антивирус включен, базы обновлены, «Контролируемый доступ к папкам» включен	3 мин

☐	Действие	Время
☐	ПИН-код на SIM-карте включен	1 мин
☐	«Стоп-кредит» установлен (себе и родителям)	5 мин
☐	Кредитная история проверена в этом квартале	5 мин
☐	Список ключей ЭЦП в кабинете НУЦ проверен	5 мин
☐	С семьей договорились о кодовом слове и правиле «перезвони»	—
☐	Я знаю, кому на работе сообщать об инциденте	—

АКАДЕМИЯ ТРУДОВОГО ПРАВА И КАДРОВЫХ КОМПЕТЕНЦИЙ HR UP SKILL

КУРС «Специалист отдела кадров»

Для тех, кто осваивает профессию, приходит в кадры из смежной сферы или хочет заново выстроить кадровый учет последовательно и системно.

Как проходит: каждую неделю — 3 живых вебинара в Zoom с разбором ваших вопросов, видеоуроки по каждой теме, практические задания, тренажеры и симуляции кадровых ситуаций, итоговые тестирования по темам, аттестация.

Что остается у вас: шаблоны документов, пошаговые алгоритмы и чек-листы, конспекты, записи всех занятий в личном кабинете на 12 месяцев.

Результат: уверенно оформляете прием, перевод, отпуск, увольнение, ведете ЕСУТД — и обосновываете каждый документ нормой ТК РК.

https://www.hrdok.kz/ok2026

КУРС «Управление трудовыми отношениями»

Для действующих кадровиков, HR, юристов и руководителей кадровых служб, которые хотят систематизировать практику и уверенно работать со сложными вопросами.

Как проходит: каждую неделю — 3 живых вебинара в Zoom, видеоуроки, разборы сложных случаев и судебной практики, внутренний аудит своей практики по контрольным листам по каждой теме.

Что остается у вас: контрольные листы внутреннего аудита, шаблоны, алгоритмы, конспекты, собственная карта кадровых рисков, записи занятий на 12 месяцев.

Результат: находите и закрываете пробелы в своей работе и аргументируете решения нормой и судебной практикой — перед руководителем, инспектором и в споре.

https://www.hrdok.kz/pravo-hr

ПРОЕКТ «КАБИНЕТ КАДРОВИКА» — вебинары и разборы весь год,
https://www.hrdok.kz/kabinet

КОНСУЛЬТАЦИОННЫЙ ПРОЕКТ «Кабинет кадровика»

Для тех, кто уже в профессии и не хочет оставаться один на один с изменениями законодательства и сложными ситуациями.

Результат: вовремя узнаете об изменениях ТК РК, разбираете реальные кейсы и всегда знаете, где спросить и на что опереться.

Внутри: вебинары каждую среду и их записи, конспекты с образцами, архив разборов, ответы на ваши вопросы в чате, Энциклопедия кадровых решений.

Доступ на 12 месяцев, вебинары каждую среду, материалы для ежедневной кадровой работы в личном кабинете.

https://www.hrdok.kz/kabinet

Цифровой кадровый аудит: ЕСУТД и Enbek.kz

Самопроверка сведений в ЕСУТД, ответы со ссылками на нормы, образцы документов и судебная практика. Доступ сразу после оплаты.

Цифровое решение работает в браузере на казахстанском сервере.

https://www.hrdok.kz/esutd

Оплата от ИП или юрлица. Рассрочки Kaspi и Halyk банка
Подобрать программу —www.hrdok.kz

Итог: пауза 20 секунд

1. **Кто просит? Зачем сейчас? Что я подтверждаю?** Три вопроса, которые останавливают почти любую схему.
2. **Код — только туда, куда вы пришли сами.** Кто просит код — тот вор.
3. **Сегодня:** облачный пароль в Telegram, двухэтапная проверка в WhatsApp, 2FA в почте, проверка устройств — себе и родителям.
4. **На работе:** Win + L, пароли не на стикере, ЭЦП не передаем, файлы с ИИН — архивом с паролем, о подозрительном — сразу.
5. **Работодателю:** не «скачанное положение», а ревизия доступов, конкретные требования, ознакомление под подпись и регулярный контроль.

МАТЕРИАЛЫ

Памятка «Кибербезопасность каждый день» — в Telegram-канале «Исповедь кадровика»: **https://t.me/hr_audit**

Запись эфира — на YouTube-канале **youtube.com/@lebed_audit**.

С уважением, Екатерина Лебедь.

Дата разработки конспекта: 06.11.2026 г.