



**МИНИСТЕРСТВО
ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ БУРЯТИЯ**

**БУРЯАД УЛАСАЙ
БОЛБОСОРОЛОЙ БОЛОН
ЭРДЭМ УХААНАЙ ЯАМАН**



Коммунистическая ул., д. 47, г. Улан-Удэ, Республика Бурятия, 670001, в/я 17.
тел. (3012) 21-49-15, 21-90-96, факс (3012) 22-01-55, URL: <http://egov-buryatia.ru/minobr/>, E-mail: minobr@govrb.ru

Дата № № *19.02.2021 г. № 02-11/571*
На № _____ от _____

Руководителям органов
местного самоуправления,
осуществляющих управление
в сфере образования

Об участии в цифровом диктанте

Руководителям государственных
общеобразовательных организаций

Министерство образования и науки Республики Бурятия информирует о проведении Министерством цифрового развития и связи Алтайского края Цифрового диктанта в области безопасности персональных данных.

Целью проведения Диктанта является повышение уровня цифровой грамотности широкого круга пользователей (студенты, госслужащие, работники коммерческих организаций) в области безопасности персональных данных, а также разбор типовых нарушений и угроз, подстерегающих пользователей при работе с персональными данными в цифровой среде.

Форма проведения: для прохождения Диктанта нужно перейти по ссылке: <https://poll.alregn.ru/diktant>, после чего пройти идентификацию в Единой системе идентификации и аутентификации (ЕСИА) при помощи своей учетной записи на Портале государственных услуг.

Перед прохождением Диктанта пользователь может ознакомиться с теоретическим материалом по персональным данным, который содержит основные положения законодательства Российской Федерации в области обработки

персональных данных, разбор реальных случаев вымогательства персональных данных, мошенничества с персональными данными и других угроз безопасности персональных данных, а также советы по обеспечению безопасности субъекта персональных данных в цифровой среде. Данный материал представлен на сайте Минцифры Алтайского края по ссылке: <https://digital.alregn.ru/important/tsifrovoy-diktant-v-oblasti-personalnykh-dannykh.php>

Приложение на 14 л.

Заместитель министра –
председатель Комитета общего
и дополнительного образования



В.А. Поздняков



**МИНИСТЕРСТВО
ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Пресненская наб., д.10, стр.2, Москва, 123112
Справочная: +7 (495) 771-8000

05.02.2021 № П18-1-06-070-3279

на № _____ от _____

О направлении информации

Высшие исполнительные органы
государственной власти субъектов
Российской Федерации

По списку

Уважаемые коллеги!

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации сообщает о проведении Цифрового диктанта в области безопасности персональных данных (далее – «Цифровой диктант»), организованного Министерством цифрового развития и связи Алтайского края совместно с Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Алтайскому краю и Республике Алтай.

Целью проведения Цифрового диктанта является повышение уровня цифровой грамотности широкого круга пользователей (студентов, госслужащих, работников коммерческих организаций) в области безопасности персональных данных, а также выявление типовых нарушений и угроз, подстерегающих пользователей при работе с персональными данными в цифровой среде.

Коллеги приглашают принять участие представителей вашего ведомства и органа исполнительной государственной власти, а также подведомственных учреждений в Цифровом диктанте (адрес в сети Интернет: <https://poll.alregn.ru/diktant>), заполнив соответствующую тестовую форму в период с 11.02.2021 по 23.02.2021.

Перед прохождением Цифрового диктанта пользователь может ознакомиться с теоретическим материалом по персональным данным, который содержит основные положения законодательства Российской Федерации в

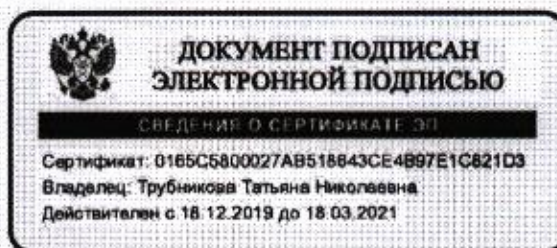
области обработки персональных данных, разбор реальных случаев
вымогательства персональных данных, мошенничества с персональными
данными и других угроз безопасности персональных данных и иные советы по
обеспечению безопасности субъекта персональных данных в цифровой среде.

Материалы для изучения также доступны на официальном сайте
Министерства цифрового развития и связи Алтайского края по ссылке:
<https://digital.alregn.ru/important/tsifrovoy-diktant.php>

Приложение: на 8 л. в 1 экз.

Директор Департамента
координации и реализации
проектов по цифровой экономике

Т.Н. Трубникова



Цифровой диктант по персональным данным.

Введение. Цифровой диктант по персональным данным (далее – «Диктант») разработан Министерством цифрового развития и связи Алтайского края и Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Алтайскому краю и Республике Алтай при поддержке Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Целью проведения Диктанта является повышение уровня цифровой грамотности широкого круга пользователей (студенты, госслужащие, работники коммерческих организаций) в области безопасности персональных данных, а также разбор типовых нарушений и угроз, подстерегающих пользователей при работе с персональными данными в цифровой среде.

Форма проведения. Для прохождения Диктанта нужно перейти по ссылке: <https://poll.alregn.ru/diktant/>, после чего пройти идентификацию в Единой системе идентификации и аутентификации (ЕСИА) при помощи своей учетной записи на Портале государственных услуг.

Перед прохождением Диктанта пользователь может ознакомиться с теоретическим материалом по персональным данным, который содержит основные положения законодательства Российской Федерации в области обработки персональных данных, разбор реальных случаев вымогательства персональных данных, мошенничества с персональными данными и других угроз безопасности персональных данных, а также советы по обеспечению безопасности субъекта персональных данных в цифровой среде. Данный материал представлен на сайте Минцифры Алтайского края по ссылке: <https://digital.alregn.ru/important/tsifrovoy-diktant.php>

Диктант состоит из 30 вопросов, для каждого вопроса предлагается 3 либо 4 варианта ответа, только один из которых верный. Время прохождения теста составляет 40 минут.

По итогам прохождения Диктанта, в случае, если получено более 75% правильных ответов, пользователю выдается цифровой сертификат об успешном прохождении теста (в электронном виде), отображается статистика ответов.

В случае, если количество правильных ответов составит менее 75%, Диктант считается не пройденным. Повторное прохождение возможно, предварительно ознакомившись с теоретической частью, представленной на сайте Минцифры Алтайского края.

ВОПРОСЫ

к Цифровому диктанту по персональным данным.

1. Основопологающим Федеральным законом в области обеспечения прав субъектов персональных данных является:

- 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- 152-ЗС «О персональных данных Алтайского края»
- 152-ФЗ «О персональных данных»
- 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»

2. Что является персональными данными?

- любая информация, относящаяся к прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)
- информация о частной жизни физического лица, доступ к которой он решил ограничить
- сведения о религиозных убеждениях, политических взглядах, расовой и национальной принадлежности субъекта персональных данных
- любые сведения независимо от формы их представления

3. Целью Федерального закона «О персональных данных» является:

- обеспечение защиты информации в Российской Федерации
- осуществление права на поиск, получение, передачу, производство и распространение информации
- обеспечение целостности персональных данных
- обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных

4. На какие отношения не распространяется действие Федерального закона «О персональных данных»?

- на отношения, возникающие при обработке персональных данных физическими лицами, исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных
- на отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну
- не распространяется на оба перечисленных варианта

5. Что из нижеперечисленного относится к персональным данным?

- никнейм на странице форума в сети Интернет
- государственный номер транспортного средства
- дата и место рождения
- марка и модель личного телефона

6. Работодатель при устройстве женщин на работу требует справку об отсутствии беременности. Законны ли действия работодателя?

- законны при наличии соответствующих условий в трудовом договоре
- законны при наличии согласия в письменной форме субъекта персональных данных на обработку своих персональных данных
- незаконны - запрещается отказывать в заключении трудового договора женщинам по мотивам, связанным с беременностью или наличием детей

7. Если при обработке персональных данных организацией нарушаются права субъекта персональных данных, куда в первую очередь ему следует обратиться за консультацией?

- в территориальный орган МВД России
- в территориальное управление Роскомнадзора
- в администрацию города / субъекта РФ

8. Относятся ли cookies-файлы к персональным данным пользователя?

- да, относятся, так как содержат набор информации, позволяющей прямо или косвенно идентифицировать субъекта персональных данных
- нет, так как по этим данным невозможно установить конкретное лицо

9. Что относится к биометрическим персональным данным?

- сведения о состоянии здоровья
- дата и место рождения
- рентгеновские или флюорографические снимки, характеризующие физиологические и биологические особенности человека.
- отпечатки пальцев, отпечатки ладони, образец голоса

10. Персональные данные – это сведения только о живом человеке или об умершем тоже?

- сведения об умершем физическом лице – тоже персональные данные
- персональные данные могут относиться только к живому человеку

11. Вправе ли физическое лицо представлять персональные данные своих близких родственников?

- да, вправе всегда
- нет, никогда
- да только при наличии письменного согласия указанных лиц
- да только при наличии письменного согласия указанных лиц либо в случаях, установленных Федеральными законами.

12. Является ли заполнение регистрационной формы на мероприятие передачей персональных данных в адрес оператора?

- да, является
- нет, не является
- да, только если мероприятие состоялось
- да, только если мероприятие состоялось в онлайн-формате

13. Попадает ли обработка персональных данных, полученных посредством систем видеонаблюдения, под действия Федерального закона «О персональных данных»?

- да, только если система видеонаблюдения используется для идентификации субъектов
- да, попадают, если система видеонаблюдения предназначена для общего наблюдения за обстановкой на объекте
- да попадает в любом случае

14. Что необходимо предпринять в первую очередь после потери банковской карты?

- сообщить об утрате в правоохранительные органы
- с помощью онлайн-банка перевести свои средства на другую банковскую карту
- сообщить по телефону горячей линии банка о произошедшем и попросить заблокировать карту
- подождать некоторое время, возможно добрые люди ее найдут и вернут, после этого обратиться в банк за выпуском новой.

15. Какой из предложенных паролей более всего соответствует требованиям безопасности?

- N0#Pel!k
- Qwerty123
- [Дата Вашего рождения]
- 12345678901

16. Подтверждение онлайн-платежа одноразовым паролем (смс-кодом) должно осуществляться на...

- на любой странице в сети «Интернет»
- на странице интернет-магазина
- на специальной странице банка или сервиса платежей, где размещен логотип платежной системы, а сама страница имеет сертификат безопасности SSL/TLS

17. Какой из предложенных форматов файла является наиболее защищенным от несанкционированного доступа?

- формат «PDF»
- формат «DOC»
- ZIP-архив с установленным паролем
- формат «RTF»

18. Вы зашли в свой аккаунт в социальной сети и обнаружили, что некоторые новые входящие сообщения прочитаны. Вы уверены, что не читали эти сообщения. Что необходимо сделать в первую очередь?

- зайти в настройки своего аккаунта и удалить его, создать новый
- выйти из аккаунта и заново зайти в него
- проверить список активных сессий в настройках аккаунта, закрыть все активные сессии, сменить пароль аккаунта
- удалить прочитанные сообщения и сменить пароль в настройках аккаунта.

19. Вы наткнулись на баннер с текстом «На этом сайте ты можешь смотреть все закрытые фотографии в профилях своих друзей в соцсетях!» и кликнули на него. Открылся сайт со всплывающим окном, куда необходимо ввести логин и пароль от Вашей страницы в социальной сети. Какими будут Ваши действия?

- введу логин и пароль и буду рассматривать закрытые фотографии
- закрою всплывающее окно и сперва изучу сайт

- введу неправильные логин и пароль, останусь на сайте
- закрою сайт, это может быть не только опасно, но и противозаконно

20. При попытке входа в свой электронный почтовый ящик вы видите следующее сообщение: «Уважаемый пользователь, ваш почтовый адрес будет заблокирован в связи с жалобой, поступившей к администрации два дня назад. Для отмены блокировки отправьте в ответном письме свои логин и пароль, ответ на контрольный вопрос, а также информацию о дате регистрации вашего почтового ящика». Отправитель сообщения подписан как «Служба модераторов сервиса». Что вы будете делать?

- отправлю все данные, чтобы мой ящик не заблокировали
- отправлю логин и ответ на контрольный вопрос, чтобы обезопасить себя от возможного взлома
- отправлю логин и информацию дату регистрации почтового ящика, чтобы обезопасить себя от возможного взлома
- ничего не буду отправлять и удалю письмо. Администраторы почтового сервиса никогда не попросят меня отправить им сообщение с моими аутентификационными данными

21. Вы находитесь в кафе с друзьями, и Вам нужно срочно перевести небольшую сумму денег родственнику. Какой из предложенных вариантов действий следует выбрать, как самый безопасный?

- вы как раз сидите в кафе с друзьями, тут есть доступ к публичной сети Wi-Fi. Можно подключиться к сети Wi-Fi, зайти в мобильный банк и перевести деньги
- отключиться от публичной сети Wi-Fi кафе, зайти в банковское приложение на телефоне посредством личного мобильного интернета, выполнить перевод
- попросить ноутбук у друга, подключиться к Wi-Fi, и перевести деньги через сайт банка

22. Имеет ли право школа собирать отпечатки пальцев воспитанников с целью их идентификации и осуществления пропуска на территорию школы?

- да, если так решило руководство школы
- да, если родители учеников проголосовали «за» на собрании, где обсуждался данный вопрос
- нет, обработка дактилоскопической информации осуществляется только в случаях, установленных Федеральным законом от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации»

23. Администрация школы установила систему распознавания лиц с целью исключения попадания на территорию школы посторонних. Законны ли действия администрации школы?

- да, законны, при наличии согласия в письменной форме от всех зарегистрированных в системе лиц
- нет, незаконны, так как обработка биометрических персональных данных несовершеннолетних не допускается
- законны, если большинство родителей учеников проголосовали «за» внедрение данной системы на собрании

24. Возможно ли работодателю привлечь работника к ответственности, если по результатам автоматизированной обработки данных выявлено, что работник не зашел на территорию организации

- да, возможно
- нет, нельзя
- да, если привлечь понятых

25. Как оператор может получить согласие субъекта на обработку его персональных данных

- только в письменной форме
- только в письменной форме или с использованием электронной подписи
- согласие на обработку персональных данных может быть дано в любой в любой позволяющей подтвердить факт его получения форме
- согласие на обработку персональных данных может быть дано в любой позволяющей подтвердить факт его получения форме (если иное не установлено федеральным законом)

26. Кто может быть оператором персональных данных?

- только государственный или муниципальный орган
- только юридическое лицо, индивидуальный предприниматель, государственный или муниципальный орган
- физическое лицо, индивидуальный предприниматель, юридическое лицо, государственный или муниципальный орган

27. Какая основная мера по предупреждению угроз защиты информации от методов «социальной инженерии» для оператора персональных данных?

- установка антивирусных программ на рабочих станциях и серверах оператора персональных данных
- разграничение доступа сотрудников оператора
- обучение сотрудников. Все работники оператора персональных данных должны быть предупреждены об опасности раскрытия конфиденциальной информации, а также возможных способах

получения доступа к информации при помощи методов «социальной инженерии»

28. Фотографическое изображение, содержащееся в личном деле работника, относят:

- к персональным данным обычной категории
- к специальной категории персональных данных
- к биометрическим персональным данным

29. Будет ли сообщение на доске объявлений в подъезде «Житель дома Иван Иванов из кв. N имеет долги по ЖКХ» считаться разглашением персональных данных этого человека?

- нет, не будет. Иван Иванов – слишком распространенное имя, чтобы по нему можно было однозначно идентифицировать конкретного человека
- да, будет. Такое объявление идентифицирует лицо
- подъезд – общественное место, можно писать на доске объявлений любую информацию

30. По закону сведения, взятые из общедоступных источников можно использовать без согласия человека. Относятся ли к таким источникам соцсети?

- соцсети – не общедоступный источник информации, нельзя обрабатывать данные без согласия лишь потому, что человек сам их опубликовал
- спорный вопрос. В законе общедоступными источниками названы справочники и адресные книги, соцсети не упоминаются
- публикация данных о себе в соцсетях делает их доступными для всех, поэтому их можно распространять без согласия субъекта персональных данных