

**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ И СВЯЗИ**

 **Приморского края**

**Приказ**

 23.01.2023 г. Владивосток пр. 40-12

**Об утверждении Положения**

**об электронном курсе «Основы безопасной работы
в информационных системах Правительства
Приморского края»**

На основании Положения о министерстве цифрового развития и связи Приморского края, утвержденного постановлением Администрации Приморского края от 1 ноября 2019 года № 721-па (в ред. Постановлений Правительства Приморского края от 17 февраля 2020 года № 126-пп, от 11 марта 2021 года № 125-пп, от 21 сентября 2021 года № 626-пп, от 14 апреля 2022 года № 243-пп)

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемое Положение об электронном курсе «Основы безопасной работы в информационных системах Правительства Приморского края» (далее - Положение).
2. Отделу по защите информации обеспечить размещение Положения, утвержденного настоящим приказом, на «Портале электронного обучения и тестирования Правительства Приморского края».
3. Краевому государственному казенному учреждению «Информационно-технологический центр Приморского края» осуществлять зачисление на электронный курс «Основы безопасной работы в информационных системах Правительства Приморского края» лиц, поступивших на государственную гражданскую службу впервые, при получении соответствующих заявок на доступ к элементам информационно-телекоммуникационной инфрастуктуры Правительства Приморского края.
4. Контроль за исполнением настоящего приказа оставляю за собой.

|  |  |
| --- | --- |
| Заместитель Председателя Правительства Приморского края –министр цифрового развития и связи Приморского края | К.Г. Волошин |

|  |  |
| --- | --- |
|  | УТВЕРЖДЕНОприказомминистерства цифрового развития и связи Приморского краяот 23.01.2023 № пр.40-12  |

**ПОЛОЖЕНИЕ**

**об электронном курсе «Основы безопасной работы
в информационных системах Правительства
Приморского края»**

**I. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Настоящее положение определяет структуру, цели, задачи и условия освоения государственными гражданскими служащими Приморского края (далее — пользователи) электронного курса «Основы безопасной работы в информационных системах Правительства Приморского края» (далее — электронный курс).

1.2. Электронный курс является объектом авторского права, исключительные права на использование которого принадлежат министерству цифрового развития и связи Приморского края. Копирование, размножение, распространение, перепечатка (целиком или частично), или иное использование материала без письменного разрешения министерства цифрового развития и связи Приморского края не допускается.

1.3. Электронный курс предназначен для повышения уровня грамотности пользователей в сфере информационных технологий, в том числе их ознакомления с основами безопасной работы в информационных системах органов исполнительной власти Приморского края, подразделений аппарата Губернатора Приморского края и Правительства Приморского края, а также корректного использования предоставляемых служебных сервисов в своей деятельности.

1.4. Технологически электронный курс выполнен в системе дистанционного обучения «MOODLE», распространяющейся на условиях открытого лицензионного соглашения, и размещен на «Портале электронного обучения и тестирования Правительства Приморского края» по адресу в сети «Интернет» «[https://sdo.primorsky.ru](https://sdo.primorsky.ru/)».

1.5. Сопровождение материалов электронного курса и организация его прохождения пользователями осуществляются министерством цифрового развития и связи Приморского края на основании подпункта 2.1.16 Положения о министерстве цифрового развития и связи Приморского края, утвержденного постановлением Администрации Приморского края от 1 ноября 2019 года
№ 721-па.

1.6. Электронный курс включен в программу наставничества, действующую в органах исполнительной власти Приморского края, аппарате Губернатора Приморского края и Правительства Приморского края, и является частью утвержденной формы индивидуальных планов адаптации лиц,
в отношении которых осуществляется наставничество.

**II. ЦЕЛИ И ЗАДАЧИ**

2.1. Целью электронного курса является ознакомление государственных гражданских служащих Приморского края с угрозами безопасности информации, актуальными для пользователя, включая выработку базовых навыков и способов защиты от них для повышения общей защищенности информационно-телекоммуникационной инфраструктуры Правительства Приморского края.

2.2. Обучение основам безопасной работы в информационных системах органов исполнительной власти Приморского края, подразделений аппарата Губернатора Приморского края и Правительства Приморского края реализуется посредством выполнения следующих задач:

- формирования у пользователя базовых теоретических основ в области информационной безопасности;

- ознакомления с нормативными правовыми актами, устанавливающими требования по защите информации, в том числе в Правительстве Приморского края;

- приобретения практических навыков и умений безопасной работы
в информационных системах и служебных сервисах, включая использование электронной почты и информационно-телекоммуникационной сети «Интернет» на рабочем месте;

- изучения порядка обращения с машинными носителями информации,
в том числе сертификатов ключа проверки электронной подписи.

**III. СОСТАВ ЭЛЕКТРОННОГО КУРСА**

3.1. Электронный курс представляет собой систематизированный набор теоретических материалов (лекций), структурированных по разделам и объединенных одной тематикой.

Каждый раздел курса направлен на поэтапное выполнение задач электронного курса для достижения определенной настоящим Положением цели и оформлен отдельным блоком. Совокупность всех разделов курса обеспечивает формирование итоговых результатов обучения.

3.2. Электронный курс состоит из следующих основных разделов и включенных в них наборов теоретических материалов (лекций).

3.2.1. Введение в информационную безопасность.

Набор лекций:

«Основные термины и определения в области информационных технологий и защиты информации»;

«Вредоносное программное обеспечение»;

«Социальная инженерия».

3.2.2. Конфиденциальная информация.

Набор лекций:

«Определение конфиденциальности информации. Перечень конфиденциальной информации, доступ к которой ограничен федеральными законами»;

«Перечень служебной информации конфиденциального характера в Правительстве Приморского края, в аппарате Губернатора Приморского края и Правительства Приморского края, в органах исполнительной власти Приморского края»;

«Правила обращения с документами ограниченного доступа, порядок их изготовления, передачи, хранения, уничтожения».

3.2.3. Персональные данные.

Набор лекций:

«Определение персональных данных и информационных систем персональных данных. Автоматизированная и неавтоматизированная обработка персональных данных»;

«Согласие субъекта персональных данных на обработку его персональных данных»;

«Правила работы с персональными данными. Способы передачи персональных данных».

3.2.4. Служебное автоматизированное рабочее место государственного гражданского служащего Приморского края.

Набор лекций:

«Состав автоматизированного рабочего места. Типовой набор программного обеспечения»;

«Архивирование и резервирование важной информации. Использование сетевых дисков»;

«Угрозы несанкционированного доступа к информационным системам при оставлении пользователем своего рабочего места и несанкционированного просмотра защищаемой информации, отображаемой на экране»;

«Подозрительная активность технических и программных средств автоматизированного рабочего места»;

«Контроль целостности технических средств автоматизированного рабочего места»;

«Угрозы безопасности при подключении к автоматизированному рабочему месту личных устройств, в том числе носителей информации».

3.2.5. Безопасное использование служебных электронных сервисов Правительства Приморского края.

Набор лекций:

«Доменная учетная запись пользователя. Учетные записи в информационных системах»;

«Служебные электронные сервисы Правительства Приморского края, доступные по умолчанию»;

«Учетные данные. Авторизация. Логин и пароль»;

«Требования к паролю: способы создания, сложность, хранение, периодичность смены, угрозы компрометации»;

«Служебная электронная почта: проверка адресата, вложения, фишинговые письма, спам, использование почтовых клиентов»;

«Безопасность в сети «Интернет»: фильтрация и запрещенные внешние сетевые ресурсы, поддельные сайты, хранение учетных данных в памяти браузера, протокол безопасного соединения, сбор сведений о посетителях»;

«Использование служебного сервиса видеоконференц-связи: платформа, управление подключенными пользователями, размещение и удаление информации файлов в личном кабинете, очистка чата сообщений»;

«Риски, связанные с обработкой служебной информации посредством сторонних ресурсов. Угрозы безопасности при использовании личной электронной почты и мессенджеров в рабочих целях».

3.2.6. Электронная подпись.

Набор лекций:

«Использование электронных подписей. Виды и принцип работы»;

«Обращение с носителями. Действия при утрате».

3.3. В разделы курса включены вопросы для самоконтроля, направленные на закрепление пройденного материала, а также выработку практических навыков применения полученных знаний в нестандартных ситуациях.

Количество вопросов для самоконтроля не превышает 3 (трех) единиц.

**IV. ИТОГОВОЕ ТЕСТИРОВАНИЕ**

4.1. Итоговое тестирование является неотъемлемой частью электронного курса, к которой допускаются пользователи после успешного завершения освоения разделов курса и прохождения вопросов для самоконтроля.

4.2. Итоговое тестирование представляет собой набор вопросов, позволяющих провести объективную оценку достигнутых результатов по итогам изучения курса.

В итоговое тестирование включаются вопросы:

- демонстрирующие изменение компетентности пользователей в рамках изученной области;

- охватывающие все содержание электронного курса, в целях оценки общего уровня усвоения материала курса.

4.3. Количество вопросов итогового тестирования составляет 20 (двадцать) единиц.

Вопросы выбираются автоматически случайным образом из базы данных вопросов. Все вопросы оцениваются одинаково, имеют равные весовые коэффициенты и уровень сложности.

4.4. Для прохождения итогового тестирования установлено ограничение по времени — 60 (шестьдесят) минут. Количество попыток пользователя для прохождения тестирования не ограничено. Интервал между попытками составляет 60 (шестьдесят) минут.

4.5. Система оценки достигнутых результатов по освоению пользователем электронного курса отражает уровень знаний на основании итогового тестирования следующим образом:

- результат тестирования 71% - 100% - тестирование пройдено успешно;

- результат тестирования 0% - 70% - тестирование не пройдено.

**V. ПОРЯДОК ПОЛУЧЕНИЯ И ПРЕКРАЩЕНИЯ
ДОСТУПА К ЭЛЕКТРОННОМУ КУРСУ**

5.1. Доступ пользователя к электронному курсу возможен только после его зачисления (регистрации) в системе дистанционного обучения «MOODLE», выполненного на «Портале электронного обучения и тестирования Правительства Приморского края».

5.2. Зачисление пользователя на электронный курс производится уполномоченным сотрудником краевого государственного казенного учреждения «Информационно-технологический центр Приморского края» при получении заявок на создание учетных записей информационной инфраструктуры для лиц, впервые поступивших на государственную гражданскую службу в органы исполнительной власти Приморского края, аппарат Губернатора Приморского края и Правительства Приморского края.

Зачисление может также осуществляться сотрудником министерства цифрового развития и связи Приморского края в рамках реализуемых мероприятий по организационно-технической защите информации.

5.3. Для работы с электронным курсом пользователю необходимо авторизоваться на «Портале электронного обучения и тестирования Правительства Приморского края» в соответствии с используемыми механизмами идентификации и аутентификации платформы.

5.4. Доступ пользователя к некоторым разделам электронного курса может быть приостановлен в связи с обновлением данных разделов, либо электронный курс может быть не доступен в целом в случае проведения профилактических работ на «Портале электронного обучения и тестирования Правительства Приморского края».

5.5. На освоение материалов курса пользователю, после его зачисления, отводится 120 дней, по истечению которых доступ пользователя к электронному курсу автоматически блокируется.

При наличии обстоятельств, препятствующих осуществлению успешного освоения электронного курса пользователем (отсутствие на гражданской службе пользователя в связи с его нахождением в ежегодном оплачиваемом отпуске или с его временной нетрудоспособностью, а также в иных случаях), доступ к электронному курсу может быть продлен.

Допускается повторное назначение пользователям электронного курса либо отдельно раздела итогового тестирования при наличии соответствующей служебной необходимости.

**VI. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

6.1. Обновление структуры курса, теоретических материалов, базы данных вопросов и других элементов электронного курса осуществляется министерством цифрового развития и связи Приморского края в случае изменения требований законодательства Российской Федерации и Приморского края в сфере информационных технологий и защиты информации, актуализации локальных нормативных правовых актов по информационной безопасности, а также по мере служебной необходимости.

6.2. Электронный курс считается освоенным пользователем по итогам изучения всех разделов курса, завершения вопросов для самоконтроля и успешного прохождения итогового тестирования.

6.3. Информация о результатах прохождения пользователями электронного курса может быть использована министерством цифрового развития и связи Приморского края в статистических или иных исследовательских целях при условии обезличивания информации, в том числе для подготовки сводных отчетов председателю Совета по информационной безопасности при Губернаторе Приморского края об уровне осведомленности в вопросах информационной безопасности государственных гражданских служащих Приморского края.

6.4. Предложения по доработке электронного курса или сообщения
о выявленных ошибках в работе электронного курса можно направлять
на электронный почтовый адрес inform@primorsky.ru либо сообщить по телефону (423) 220-52-80.

\_\_\_\_\_\_\_\_\_\_\_