УТВЕРЖДЕНО

Приказом ГБУ КО «РПЦ»

от «16» июня 2023 г.

№ 115

РЕГЛАМЕНТ

по обеспечению информационной безопасности персональных данных в информационных системах персональных данных в государственном бюджетном учреждении Калининградской области «Региональный перинатальный центр»

г. Калининград

2023 г.

1. Общие положения

Настоящий Регламент разработан в соответствии с Федеральным законом №152-ФЗ от 27.07.2006 г. «О персональных данных», Приказом ФСТЭК России №21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и определяет обязанности, права и ответственность пользователя в информационных системах персональных данных (далее – ИСПДн) в государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр».

Допуск пользователя к работе в ИСПДн осуществляется согласно списку пользователей, утвержденному приказом главного врача. Полномочия доступа пользователя к программным и техническим средствам настраиваются Ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – Ответственный за обеспечение безопасности ПДн в ИСПДн) согласно разрешительной системе доступа к ИСПДн.

Обязанности по установке, настройке, администрированию информационных систем государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр» возложены на Ответственного за обеспечение безопасности ПДн в ИСПДн.

Настоящий Регламент является дополнением к действующим нормативным правовым актам Российской Федерации по вопросам безопасности информации и не исключает обязательного выполнения их требований.

2. Права и обязанности пользователя ИСПДн

Перед началом работы пользователь обязан убедиться в целостности технических средств ИСПДн и отсутствии посторонних лиц.

Для входа в систему пользователь обязан ввести личные атрибуты доступа, полученные у Ответственного за обеспечение безопасности ПДн в ИСПДн. После успешного процесса аутентификации пользователю будут доступны информационные ресурсы согласно разрешительной системе доступа.

Обработка информации осуществляется пользователем при помощи установленного прикладного программного обеспечения в рамках технологического процесса обработки защищаемой информации.

На время оставления рабочего места пользователь блокирует ИСПДн средствами защиты от несанкционированного доступа.

По завершении работ пользователь должен завершить сеанс работы с прикладным программным обеспечением и выключить автоматизированное рабочее место.

При работе с ИСПДн пользователь обязан:

– знать и соблюдать установленные требования по защите персональных данных, учету, хранению и пересылке носителей информации, а также руководящих и организационно-распорядительных документов (Положение о защите и обработке персональных данных, инструкции, приказы и другие локальные акты государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр» касаемо его должностных обязанностей);

– использовать для работы только учтенные в установленным порядком съемные носители информации;

– проверять перед началом обработки на автоматизированном рабочем месте (далее –АРМ) файлы, хранящиеся на съемных носителях информации, на наличие вредоносных программ;

– соблюдать утвержденную разрешительную систему доступа пользователей к ресурсам ИСПДн;

– хранить в тайне персональные данные (далее – ПДн), ставшие известными при выполнении должностных обязанностей, пресекать действия других лиц, которые могут привести к разглашению данной информации;

– никому не сообщать свои персональные атрибуты доступа к ИСПДн (имя пользователя, пароль).

– получать и использовать персональные атрибуты доступа согласно положениям настоящего Регламента;

– осуществлять антивирусный контроль согласно положениям настоящего Регламента;

– расположить устройство вывода информации таким образом, чтобы исключить возможность несанкционированного просмотра выводимой на экран информации;

– незамедлительно докладывать Ответственному за обеспечение безопасности ПДн в ИСПДн о:

- фактах совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к АРМ;
- несанкционированных (произведенных с нарушением установленного порядка) изменениях в конфигурации программных или аппаратных средств ИСПДн;
- некорректном функционировании установленных на АРМ технических средств защиты;

- сообщениях системы антивирусной защиты обо всех угрозах заражения АРМ;
- фактах несанкционированных изменений в конфигурации технических и программных средств, некорректной работы средств защиты, нарушений правил работы с ИСПДн другими пользователями.

Пользователю запрещается:

– использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;

– оставлять включенными без присмотра средства вычислительной техники, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации – об обнаружении такого рода ошибок ставить в известность Ответственного за обеспечение безопасности ПДн в ИСПДн;

– передавать информацию о сетевом имени, пароле и правах доступа другим лицам, если это не вызвано служебной необходимостью;

– использовать локальные и сетевые диски компьютера для хранения данных, не относящихся к служебной деятельности.

– оставлять во время работы носители информации без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка информации;

– записывать и хранить ПДн на неучтенных установленным порядком носителях информации;

– производить копирование отдельных файлов с учтенных носителей информации на неучтенные носители информации, в том числе для временного хранения информации;

– хранить на учтенных носителях информации программы и данные, не относящиеся к рабочей информации;

– отключать (блокировать) средства защиты информации;

– оставлять бесконтрольно запущенные сеансы работы с ПДн;

– привлекать посторонних лиц для производства ремонта АРМ;

– входить в операционную систему под учетной записью администратора.

Пользователь имеет право:

– в отведенное время работать с ИСПДн в рамках поставленных задач и должностных обязанностей в соответствии с установленной технологией обработки информации и полномочиями доступа к защищаемой информации, присвоенными Ответственным за обеспечение безопасности ПДн в ИСПДн;

– обращаться к Ответственному за обеспечение безопасности ПДн в ИСПДн с просьбой об оказании технической и методической помощи в работе и по обеспечению безопасности информации.

3. Порядок допуска сотрудников к работе в ИСПДн

Для допуска к персональным данным работник обязан ознакомится с организационной распорядительной документацией государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр», определяющей порядок работы с ПДн в ИСПДн.

Ответственный за обеспечение безопасности ПДн в ИСПДн настраивает права учетной записи пользователя для доступа к персональным данным, обрабатываемым в информационной системе, вносит необходимые изменения в матрице доступа к информационной системе и вносит изменения в список лиц, допущенных к работе с персональными данными, который утверждается приказом главного врача государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр».

По умолчанию подключаемый пользователь наделяется минимальным набором прав по управлению операционной средой компьютера и его конфигурацией. Повышение уровня прав осуществляется на основании заявки или на основании служебной записки, оформленной в произвольной форме на имя Ответственного за обеспечение безопасности ПДн в ИСПДн с обоснованием требуемых изменений. Максимально возможным уровнем доступа для пользователя информационной системы является включение в группу локальных администраторов. Исключением из данного правила являются служебные учетные записи, применяемые в целях администрирования информационной системы.

4. Порядок установки, настройки и использования ПО

Первоначальная комплектация АРМ в части программного обеспечения определяется Ответственным за обеспечение безопасности ПДн в ИСПДн. Программное обеспечение, не входящее в состав АРМ, не может быть установлено и использовано работниками государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр» без процедуры согласования с Ответственным за обеспечение безопасности ПДн в

ИСПДн. Установку и настройку программного обеспечения может осуществлять только Ответственный за обеспечение безопасности ПДн в ИСПДн.

На АРМ государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр» разрешается устанавливать и использовать только лицензионное программное обеспечение.

Программное обеспечение государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр» используется работниками исключительно для выполнения ими своих служебных обязанностей.

В случаях некорректной работы программных продуктов или сбоев работники обязаны незамедлительно обратиться к Ответственному за обеспечение безопасности ПДн в ИСПДн.

Работникам запрещается:

– устанавливать самостоятельно программное обеспечение;

– вносить изменения в установленное программное обеспечение (включая обновление версии продукта);

– удалять программное обеспечение;

– использовать установленное программное обеспечение в целях, не связанных со служебной деятельностью.

5. Организация парольной защиты

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на АРМ, контроль действий пользователей при работе с паролями возлагается на Ответственного за обеспечение безопасности ПДн в ИСПДн.

Личные пароли должны генерироваться пользователями ИСПДн самостоятельно с учетом следующих требований:

– длина пароля должна быть не менее 6 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах и цифры;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, учётную запись пользователя, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 1 позиции;

– личный пароль пользователь обязан хранить в тайне.

Административные пароли должны генерироваться Ответственным за обеспечение безопасности ПДн в ИСПДн с учётом всех требований к личным паролям, за исключением длины и алфавита пароля: длина должна составлять не

менее 10 символов, а в символах пароля – присутствовать специальные (/, *, -, +, @, #, $, %, ^, & и т.д.).

В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Ответственного за обеспечение безопасности ПДн в ИСПДн.

Смена паролей должна проводиться не реже одного раза в 120 дней.

Внеплановая смена всех администраторских паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр» и другие обстоятельства) администраторов и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем ИСПДн.

В случае компрометации пароля пользователя информационной системы должны быть немедленно предприняты меры по смене пароля в соответствии с настоящим Регламентом.

При увольнении сотрудника действие соответствующей учетной записи приостанавливается.

Пользователям и Ответственному за обеспечение безопасности ПДн в ИСПДн запрещается:

– записывать пароли и хранить их в местах, где с ними могут ознакомиться посторонние лица (помечать его на мониторе);
– хранить пароли в записанном виде на отдельных листах бумаги;
– сообщать свои пароли посторонним лицам;
– повторно устанавливать ранее использованные пароли.

6. Организация антивирусной защиты

Установка и настройка параметров средств антивирусного контроля на АРМ осуществляется Ответственным за обеспечение безопасности ПДн в ИСПДн.

Обновление антивирусных баз осуществляется автоматически при подключении АРМ к сети.

Полная антивирусная проверка АРМ должна осуществляется автоматически один раз в неделю. Ответственный за обеспечение безопасности ПДн в ИСПДн контролирует проведение и результаты таких проверок.

Пользователю запрещается отключать или останавливать постоянную защиту антивирусной программы.

При возникновении подозрения на наличие вредоносного ПО (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и

т.п.) пользователь самостоятельно или вместе с Ответственным за обеспечение безопасности ПДн в ИСПДн должен провести внеочередной антивирусный контроль своего рабочего места.

При обнаружении вредоносного ПО пользователь обязан:

– прекратить какие-либо действия по обработке информации на АРМ;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Ответственного за обеспечение безопасности ПДн в ИСПДн, владельца зараженных файлов, а также других сотрудников, использующих эти файлы в работе;

– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

– по факту обнаружения зараженных вирусом файлов в ИСПДн Ответственным за обеспечение безопасности ПДн в ИСПДн выявляется предположительный источник (отправитель, владелец и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса с целью предотвращения его распространения в государственном бюджетном учреждении Калининградской области «Региональный перинатальный центр».

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, оптических дисках, флэш носителях и т.п.). Разархивирование и антивирусный контроль входящей информации необходимо проводить непосредственно после ее приема в ИСПДн. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив файлового сервера должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц. Плановые проверки компьютеров пользователей проводятся еженедельно.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено Ответственным за обеспечение безопасности ПДн в ИСПДн на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети) должна быть выполнена антивирусная проверка на ПК Ответственным за обеспечение безопасности ПДн в ИСПДн.

7. Порядок работы в локальной сети и сети Интернет

Пользователи локальной сети обязаны:

– соблюдать правила работы в локальной сети, оговоренные настоящим Регламентом;

– при доступе к общим ресурсам локальной сети соблюдать правила, установленные Ответственным за обеспечение безопасности ПДн в ИСПДн для используемых ресурсов;

– немедленно сообщать Ответственному за обеспечение безопасности ПДн в ИСПДн об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящего Регламента кем-либо;

– Ответственный за обеспечение безопасности ПДн в ИСПДн при необходимости с помощью других специалистов должен провести расследование указанных фактов и принять соответствующие меры;

– немедленно отключать от локальной сети АРМ, который подозревается в заражении вирусом. АРМ не должен подключаться к сети до тех пор, пока Ответственный за обеспечение безопасности ПДн в ИСПДн не удостоверится в удалении вируса;

– выполнять предписания Ответственного за обеспечение безопасности ПДн в ИСПДн, направленные на обеспечение безопасности локальной сети;

– в случае обнаружения неисправности оборудования или программного обеспечения пользователь должен обратиться к Ответственному за обеспечение безопасности ПДн в ИСПДн.

Пользователи сети имеют право:

– использовать в работе предоставленные им сетевые ресурсы в предусмотренных настоящим Регламентах рамках, если иное не предусмотрено по согласованию с Ответственным за обеспечение безопасности ПДн в ИСПДн;

– обращаться к Ответственному за обеспечение безопасности ПДн в ИСПДн по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов или влияющие на загруженность или безопасность системы, должны санкционироваться Ответственным за обеспечение безопасности ПДн в ИСПДн.

Пользователям сети запрещено:

– использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей без согласования с Ответственным за обеспечение безопасности ПДн в ИСПДн;

– самостоятельно устанавливать или удалять сетевые программы на АРМ, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов;

– самовольно подключать АРМ к сети, а также изменять IP-адрес компьютера. Передача данных в сеть с использованием других IP-адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других АРМ;

– Использовать иные формы доступа из ИСПДн к сети Интернет, за исключением разрешенных Ответственным за обеспечение безопасности ПДн в ИСПДн;

– осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках;

– пользователи должны уважать право других пользователей на личную информацию. Это означает, что пользователь не имеет права пользоваться чужими именами и паролями для входа в сеть, читать чужую почту, причинять вред данным, принадлежащим другим пользователям.

Работа с корпоративной электронной почтой

– Корпоративная электронная почта предоставляется сотрудникам только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.

– Все электронные письма, создаваемые и хранимые в корпоративной почте, являются собственностью государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр» и не считаются персональными.

– Входящие письма должны проверяться на наличие вирусов или других вредоносных программ.

– Вся информация, составляющая ПДн государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр», при передаче через открытые сети, такие как Интернет, должна быть предварительно зашифрована.

При работе с корпоративной электронной почтой запрещается:

– использовать адрес корпоративной почты для оформления подписок без предварительного согласования с Ответственным за обеспечение безопасности ПДн в ИСПДн;

– публиковать свой адрес либо адреса других сотрудников компании на общедоступных Интернет ресурсах (форумы, конференции и т.п.);

– выполнять работы, не предусмотренные технологией обработки информации и должностными обязанностями пользователей;

– запрещено открывать или запускать приложения, полученные по корпоративной электронной почте от неизвестного источника и (или) не затребованные пользователем;

– запрещено осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

Работа с сетью Интернет

– Пользователи используют программы для поиска информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей.

– Использование ресурсов сети Интернет разрешается только в рабочих целях, использование ресурсов не должно потенциально угрожать государственному бюджетному учреждению Калининградской области «Региональный перинатальный центр».

– Действия любого пользователя, подозреваемого в нарушении правил пользования сетью Интернет, могут быть запротоколированы и использованы для принятия решения о применении к нему дисциплинарных взысканий.

– Все программы, используемые для доступа к сети Интернет, должны быть одобрены Ответственным за обеспечение безопасности ПДн в ИСПДн.

– В государственном бюджетном учреждении Калининградской области «Региональный перинатальный центр» должен вестись список запрещенных сайтов. Программы для работы с сетью Интернет должны быть сконфигурированы так, чтобы к этим сайтам нельзя было получить доступ.

При работе с ресурсами Интернет запрещается:

– загружать и запускать исполняемые либо иные файлы без предварительной проверки антивирусным программным обеспечением на наличие вредоносных программ;

– использовать анонимные прокси-серверы;

– использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию локальными нормативными актами государственного бюджетного учреждения Калининградской области «Региональный перинатальный центр».

8. Ответственность пользователя

Пользователи несут ответственность за нарушения требований нормативных правовых актов Российской Федерации в области обработки и обеспечения безопасности информации и настоящего Регламента. Пользователь при работе в ИСПДн отвечает за:

– правильность и полноту выполнения целей, задач, функций, прав и обязанностей, возложенных на него;

– сохранность и работоспособное состояние технических и программных средств, средств защиты ИСПДн (в рамках своего рабочего места);

– сохранность защищаемой информации и персональных атрибутов доступа.

9. Заключительные положения

Все работники, обрабатывающие персональные данные, должны быть предупреждены об ответственности (Приложение №1) и ознакомлены под подпись с перечисленными выше требованиями.

Приложение №1
к Регламенту по обеспечению
информационной безопасности
ПДн в ИСПДн

Выдержки из статей Уголовного кодекса РФ
Памятка пользователю ИСПДн

– *Статья 272. Неправомерный доступ к компьютерной информации*

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации,

- наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности,

-наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода, осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения,

- наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления,

- наказываются лишением свободы на срок до семи лет.

– *Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ*

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации,

- наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности,

- наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления,

- наказываются лишением свободы на срок до семи лет.

– *Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.*

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб,

- наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления,

- наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

– *Статья 293. Халатность*

Халатность, то есть неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе, если это повлекло существенное нарушение прав и законных интересов граждан или организаций, либо охраняемых законом интересов общества или государства,

- наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до трех месяцев.