УТВЕРЖДЕНА
приказом ФПК «Фонд капитального ремонта многоквартирных домов Приморского края»
от 16.12.2021 № 05/131 п

приложение к приказу № 2

# ПОЛИТИКА

## информационной безопасности в ФПК «Фонд капитального ремонта многоквартирных домов Приморского края»

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика информационной безопасности (далее - Политика) утверждается генеральным директором ФПК «Фонд капитального ремонта многоквартирных домов Приморского края» и определяет мероприятия, процедуры и правила по защите информации в информационных системах ФПК «Фонд капитального ремонта многоквартирных домов Приморского края».

1.2. Положения настоящей Политики распространяются на следующие информационные системы ФПК «Фонд капитального ремонта многоквартирных домов Приморского края»:

– сегмент ИС «РСМЭД»;

– ИСПДн «Фонд капитального ремонта многоквартирных домов Приморского края».

1.3. Положения настоящей Политики обязательны к исполнению для всех пользователей указанных в п. 1.2 информационных систем (далее - Пользователи), а также для администраторов безопасности и системных администраторов (далее - Администраторы).

1.4. В соответствии с приказом Президента Российской Федерации № 188 от 6 марта 1997 года к сведениям конфиденциального характера (защищаемой информации) в ФПК «Фонд капитального ремонта многоквартирных домов Приморского края» относятся:

– сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

– сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами;

– служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

– сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

1.5. Целями настоящей Политики являются:

– обеспечение конфиденциальности, целостности, доступности защищаемой информации;

– предотвращение утечек защищаемой информации;

– мониторинг событий безопасности и реагирование на инциденты безопасности;

– нейтрализация актуальных угроз безопасности информации;

– выполнение требований действующего законодательства по защите информации.

1.6. В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и

определения, установленные национальными стандартами в области защиты информации.

1.7. Настоящая Политика разработана с учетом положений следующих законодательных и нормативно-правовых актов:

– Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;

– Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;

– «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;

– «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;

– методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;

– «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;

– «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

## 2. ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ ОБРАБОТКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

2.1. В данном разделе настоящей Политики описаны технологические процессы обработки различных видов защищаемой информации в информационных системах ФПК «Фонд капитального ремонта многоквартирных домов Приморского края». Администраторы и Пользователи, допущенные к обработке той или иной защищаемой информации, обязаны производить обработку этой информации в соответствии с соответствующими описаниями технологических процессов обработки информации, приведенных в данном разделе.

2.2. Технологический процесс обработки защищаемой информации в информационных системах (Далее – ИС) ФПК «Фонд капитального ремонта многоквартирных домов Приморского края»:

Сегмент ИС «РСМЭД» состоит из 81 автоматизированного рабочего места, имеющих одноточечный выход в сети общего пользования и международного телекоммуникационного обмена. Задачей автоматизированного рабочего места является взаимодействие с сегментом ИС «РСМЭД» посредством веб-интерфейса в целях обеспечения деятельности по автоматизации процессов делопроизводства внутреннего и межведомственного взаимодействия между ФПК «Фонд капитального ремонта многоквартирных домов Приморского края» и министерствами Правительства Приморского края,

и муниципальными образованиями Приморского края. Файлы с данными формируются при помощи прикладного программного обеспечения или передаются из иных информационных систем на учтенных съемных носителях информации. Для передачи защищаемой информации в сегменте ИС «РСМЭД» согласно «Техническим требованиям на подключение к ИС «РСМЭД», утвержденным КГБУ «ИТЦ Приморского края», используется средство криптографической защиты информации «программный комплекс ViPNet Client»

ИСПДн «Фонд капитального ремонта многоквартирных домов Приморского края» состоит из 81 автоматизированного рабочего места, имеющих одноточечный выход в сети общего пользования и международного телекоммуникационного обмена. Задачей автоматизированного рабочего места является автоматизация процессов кадрового и бухгалетрского учета и деятельности Фонда.

## 3. ПРАВИЛА И ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИС, ПОЛИТИКА РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ИС

3.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику ФПК «Фонд капитального ремонта многоквартирных домов Приморского края», допущенному к работе с ресурсами ИС присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

3.2. Под учетной записью Пользователя понимается учетная запись для доступа к информационной системе.

3.3. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) в ИС запрещено.

3.4. Процедура регистрации пользователя ИС для сотрудника ФПК «Фонд капитального ремонта многоквартирных домов Приморского края», и

предоставления ему (или изменения его) прав доступа к ресурсам ИС инициируется заявкой руководителя подразделения, в котором работает этот сотрудник. Форма заявки приведена в Приложении № 1 к настоящей Политике. В заявке указывается:

– содержание запрашиваемых изменений (регистрация нового пользователя ИС, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИС ранее зарегистрированного пользователя);

– должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;

– полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИС);

– заявку визирует администратор безопасности, утверждая тем самым возможность допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных задач ресурсам ИС.

3.5. Администратор перед визированием заявки осуществляет верификацию пользователя (подтверждает его личность), а также уточняет его должностные и функциональные обязанности и сопоставляет их с технологическими процессами обработки информации, описанным в разделе 2 настоящей Политики. Допуск Пользователей к обработке информации в ИС производится на основании завизированной Администратором заявки, составленной по форме, приведенной в Приложении № 1 к настоящей Политике. При визировании очередной заявки Администратор осуществляет актуализацию следующих документов:

– положение о разграничении прав доступа в ИС (при необходимости, Приложение № 2 к настоящей Политике);

– Перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами ИС (Приложение № 3 к настоящей Политике).

3.6. После визирования заявки Администратор определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная, учетная запись приложения, временная, гостевая) и производит необходимые настройки СЗИ от НСД и формирует учетную запись и первичный пароль. Дает ознакомиться с инструкцией Пользователя ИС под роспись, сообщает пользователю идентификационные данные и допускает к работе в ИС. После допуска к работе в ИС, Пользователь самостоятельно формирует пароль доступа к своей учетной записи в соответствии с требованиями раздела 3 Инструкции Пользователя ИС.

3.7. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания. Исполненная заявка хранится у Администратора и может быть использована для восстановления полномочий пользователей после сбоев в работе ИС, а также для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИС при разборе инцидентов безопасности.

3.8. Для проведения временных работ в ИС сотрудниками сторонних организаций предусмотрена гостевая временная учетная запись «Guest». Данная учетная запись отключена и активируется (наделяется необходимыми полномочиями) только при необходимости. Все работы от имени такой учетной записи проводятся только под контролем Администратора.

3.9. В качестве модели разграничения доступа к ресурсам ИС выбрана ролевая модель. Пользователям назначается роль в разграничительной системе ИС в зависимости от выполняемых должностных обязанностей и задач и, соответственно, в зависимости от необходимости по доступу к тем или иным ресурсам ИС. Обязанности и задачи пользователей определяются исходя из технологических процессов обработки информации, описанных в разделе 2 настоящей Политики. Описание всех возможных ролей в ИС приведено в Приложении № 2 к настоящей Политике. Помимо учетных записей Пользователей доступ к системе получают различные системные службы и процессы.

3.10. Перечень лиц, их должностей, а также служб и процессов, допущенных к работе с ресурсами ИС и сопоставляемые им роли приведены в Приложении № 3 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.

3.11. Перечень помещений, в которых разрешена работа с ресурсами ИС, расположены технические средства ИС, а также перечень лиц, допущенных в эти помещения приведен в Приложении № 4 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.

3.12. Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только администраторам безопасности, системным администраторам и сотрудникам сторонней организации, производящим работы в сети ФПК «Фонд капитального ремонта многоквартирных домов Приморского края» на договорной основе под контролем Администратора. При вводе в эксплуатацию сетевого оборудования на нем обязательно меняются идентификационные и аутентификационные данные, установленные производителем устройства по умолчанию. Новые идентификационные данные на сетевых устройствах должны соответствовать установленной парольной политике.

3.13. Пользователям запрещены любые действия в ИС до прохождения процедуры идентификации и аутентификации в системе. Администратору разрешается ряд действий до прохождения идентификации и аутентификации в ИС в ряде случаев. Условия, при которых разрешаются такие действия и перечень разрешенных действий для Администратора до прохождения процедуры идентификации и аутентификации в ИС перечислены в пункте 5.9 инструкции Администратора.

# 4. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ

4.1. С целью определения разрешенных маршрутов прохождения информации между пользователями, устройствами, сегментами в рамках ИС, а также между информационными системами и при взаимодействии с сетью Интернет устанавливаются правила и процедуры управления информационными потоками.

4.2. С целью управления информационными потоками внутри периметра защищаемой сети ФПК «Фонд капитального ремонта многоквартирных домов Приморского края» на всех сетевых устройствах (включая сетевые адаптеры АРМ Пользователей и серверов) прописываются статические маршруты. Перечень статических маршрутов приведен в Приложении № 5 к настоящей Политике.

4.3. Администратор осуществляет контроль неизменности статических маршрутов, а также добавляет необходимые маршруты в случае необходимости и документирует изменения.

4.4. Контроль и фильтрация информационных потоков между ИС и внешними телекоммуникационными сетями осуществляется с помощью межсетевого экрана ViPNet Client 4.

4.5. Для контроля и фильтрации информационных потоков между ИС и внешними телекоммуникационными сетями выбирается политика «Блокировать все, кроме явно разрешенного». Такая политика выбрана с целью исключения возможности доступа Пользователей к сайтам с вредоносным содержимым, а также к фишинговым сайтам (сайты, имитирующие другие легальные сайты с целью кражи аутентификационной и/или личной информации Пользователей). Также такая политика выбрана исходя из практической невозможности блокировки всех фишинговых сайтов и ресурсов с вредоносным содержимым при выборе политики «Разрешено все, кроме явно запрещенного».

4.6. С целью реализации политики контроля и фильтрации информационных потоков между ИС и внешними телекоммуникационными сетями «Блокировать все, кроме явно разрешенного» утверждается список разрешающих правил взаимодействия с внешними телекоммуникационными сетями, приведенный в Приложении № 6 к настоящей Политике. Данный список может быть дополнен на основании служебной записки Администратору с указанием обоснования добавления того или иного ресурса/сайта/протокола/порта в список разрешенных.

4.7. Администратор обеспечивает соответствие настроек межсетевого экрана ViPNet Client 4, приведенному в Приложении № 6 к настоящей Политике списку разрешительных правил.

## 5. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ УСТАНОВКОЙ (ИНСТАЛЯЦИЕЙ) КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

5.1. В ИС разрешено использование только того программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования информационной системы, а также необходимы для выполнения служебных (должностных) обязанностей пользователями.

5.2. Перечень разрешенного программного обеспечения в ИС определен в Приложении № 7 к настоящей Политике.

5.3. Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только системными администраторами или администратором безопасности в соответствии с Приложением № 7. Пользователям запрещена установка любого программного обеспечения (далее - ПО) в ИС.

5.4. Пользователь имеет право подать заявку в виде служебной записки на включение в список разрешенного в ИС программного обеспечения, необходимых ему для выполнения служебных (должностных) обязанностей программ, утилит, драйверов. В такой служебной записке обязательно

указывается обоснование необходимости включения в этот список нового программного обеспечения. Срок рассмотрения заявки должен составлять не более 3 рабочих дней.

5.5. Администратор ежемесячно с помощью инструмента XSpider 7.8.25 проводит проверку соответствия состава программного обеспечения в ИС списку разрешенного ПО. В случае выявления постороннего программного обеспечения, созывается группа реагирования на инциденты информационной безопасности, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

## 6. ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, КОНТРОЛЬ ИНТЕРФЕЙСОВ ВВОДА-ВЫВОДА, ГАРАНТИРОВАННОЕ УНИЧТОЖЕНИЕ ИНФОРМАЦИИ

6.1. Одной из основных целей злоумышленников являются машинные носители информации, используемые в ИС для хранения и обработки защищаемой информации. Исходя их этого, защита машинных носителей информации (как в стационарных АРМ и серверах, так и мобильных/съемных) является ключевым звеном политики информационной безопасности ФПК «Фонд капитального ремонта многоквартирных домов Приморского края».

6.2. Учет машинных носителей осуществляется Администратором в соответствующих журналах. Администратор несет ответственность, за достоверность и своевременность сведений, отраженных в журнале учета машинных носителей информации.

6.3. В ФПК «Фонд капитального ремонта многоквартирных домов Приморского края» учету подлежат:

– съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные подобные устройства);

– портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны,

цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

– машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

6.4. Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

6.5. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

6.6. Администратор маркирует съемные машинные носители и портативные вычислительные устройства, использование которых разрешено за пределами контролируемой зоны и информационной системы и делает соответствующую отметку в журнале. Использование немаркированного соответствующим образом носителя информации за пределами контролируемой зоны и/или информационной системы является инцидентом информационной безопасности и расследуется в установленном порядке.

6.7. Использование неучтенных съемных носителей и/или портативных устройств (в том числе личных) в ИС запрещено.

6.8. Невозможность использования неучтенных съемных носителей информации обеспечивается путем программных настроек СЗИ от НСД «Dallas Lock 8.0-K». Настройками «Dallas Lock 8.0-K» неучтенные носители информации блокируются на всех стационарных устройствах ИС. Попытки использования неучтенных съемных носителей информации фиксируются

средствами «Dallas Lock 8.0-K». Такие попытки являются инцидентами безопасности и расследуются в установленном порядке.

6.9. Невозможность использования неучтенных портативных вычислительных устройств обеспечивается путем организации аутентификации в системе не только пользователя ИС, но и самого устройства по нескольким параметрам (имя устройства, IP-адрес, MAC-адрес и другие).

6.10. Невозможность использования неучтенных машинных носителей в стационарных устройствах обеспечивается путем физического контроля доступа в соответствии с инструкциями Пользователя и Администратора, а также путем проведения периодических мероприятий по инвентаризации ресурсов ИС и комплектности технических средств.

6.11. К устройствам ввода в ИС относятся: клавиатуры, мыши, сканеры, веб-камеры, кард-ридеры, сенсорные экраны (панели) и другие устройства. К устройствам ввода допущены все легальные пользователи информационной системы. Допуск к тем или иным устройствам ввода организовывается Администратором, в зависимости от выполняемых пользователем должностных обязанностей. Дополнительный контроль устройств ввода не осуществляется.

6.12. К интерфейсам ввода/вывода относятся: USB-порты, LPT-порты, COM-порты, порты вывода видеоизображения (VGA, DVI, HDMI), сетевые адаптеры (порт RJ45), гнезда вывода аудиоинформации, беспроводные адаптеры.

6.13. Сетевой трафик контролируется межсетевым экраном ViPNet Client 4 в соответствии с установленными настоящей Политикой правилами.

6.14. Порты вывода видеоизображения дополнительному контролю в ИС «АИСТ» не подлежат

6.15. Гарантированное уничтожение (стирание) информации на машинных носителях организовывается Администратором в случаях:

– возвращения учтенного съемного носителя информации Администратору;

– при вводе в эксплуатацию нового машинного носителя или технического средства со встроенными носителями информации;

– при передаче носителя информации в сторонние организации (в том числе и для проведения ремонта технического средства);

– при утилизации технических средств.

6.16. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации. Контроль невозможности восстановления уничтоженной информации производится Администратором с помощью специализированных утилит по восстановлению информации.

6.17. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации. Контроль невозможности восстановления уничтоженной информации производится Администратором с помощью специализированных утилит по восстановлению информации.

6.18. При возвращении учтенного съемного носителя информации Пользователем, а также при вводе в эксплуатацию нового машинного носителя, информация уничтожается путем использования механизма СЗИ от НСД «Dallas Lock 8.0-K» затирания файлов случайной битовой последовательностью.

6.19. При передаче носителя информации в сторонние организации (не с целью передачи на нем информации), в том числе и для ремонта носителя или технического средства, информация уничтожается путем полной многократной перезаписи машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации. Затем производится очистка всего физического пространства накопителя, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя.

6.20. В случаях уничтожения информации способами, описанными в настоящей Политики, Администратор фиксирует факт уничтожения

информации, а также факт контроля уничтожения информации в Журнале учета мероприятий по контролю обеспечения защиты информации в информационных системах Фонда.

6.21. При утилизации технических средств, а также при возникновении необходимости уничтожения информации на неперезаписываемых машинных носителях (например, CD-R), физически уничтожается сам машинный носитель.

6.22. В случае физического уничтожения машинного носителя информации, составляется акт уничтожения. Акт уничтожения машинных носителей подписывается назначенной приказом генерального директора комиссией по уничтожению персональных данных и по форме утвержденного акта уничтожения персональных данных.

## 7. УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ СТОРОННИХ ОРГАНИЗАЦИЙ (ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ)

7.1. Администратор обеспечивает доступ пользователей внешних информационных систем к ресурсам информационных систем ФПК «Фонд капитального ремонта многоквартирных домов Приморского края» в соответствии с правилами и процедурами, описанными в разделе 3 настоящей Политики. Администратор обеспечивает управление информационными потоками при взаимодействии с внешними информационными системами в соответствии с правилами и процедурами, описанными в разделе 4 настоящей инструкции.

7.2. Порядок обработки, хранения и передачи информации с использованием внешних информационных систем определяются технологическими процессами обработки информации, описанными в разделе 2 настоящей Политики.

7.3. Доступ к информационной системе авторизованными (уполномоченными) пользователями внешних информационных систем и

разрешение обработки, хранения и передачи информации с использованием внешних информационных систем в ФПК «Фонд капитального ремонта многоквартирных домов Приморского края» возможно только при выполнении следующих условий:

– при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;

– при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

## 8. ПРАВИЛА И ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ, АНАЛИЗА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

8.1. В ФПК «Фонд капитального ремонта многоквартирных домов Приморского края» в качестве средства выявления уязвимостей используется сертифицированный сканер уязвимостей XSpider 7.8.25.

8.2. Администратор не реже одного раза в месяц проводит полное сканирование системы на выявление уязвимостей. В случае поступления информации из новостных источников об уязвимостях в операционных системах и/или прикладном программном обеспечении применяемых в ИС производится внеплановое обновление базы данных сканера уязвимостей и полное сканирование информационной системы.

8.3. Администратор изучает отчеты по результатам сканирования и принимает решение о немедленном устранении выявленных уязвимостей, либо о включении мероприятий по устранению выявленных уязвимостей в план мероприятий по защите информации, в случае если выявленные уязвимости не являются критичными, или если есть возможность сделать невозможным их эксплуатацию потенциальным злоумышленником (например, путем отключения отдельных АРМ и/или сегментов сети от Интернет). При

необходимости, для адекватного реагирования на вновь выявленные угрозы может созываться ГРИИБ.

8.4. Критичность уязвимостей может быть установлена как на основании рейтинга уязвимости по шкале CVSS, так и на основании оценки рисков информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

8.5. При выявлении уязвимостей, Администратор анализирует системные журналы и журналы средств защиты информации, на предмет выявления эксплуатации выявленной уязвимости в информационной системе и последствий такой эксплуатации.

8.6. В случае невозможности оперативного устранения критичной уязвимости, Администратор уведомляет об этом генерального директора ФПК «Фонд капитального ремонта многоквартирных домов Приморского края».

## 9. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

9.1. С целью противодействия эксплуатации известных уязвимостей, в ФПК «Фонд капитального ремонта многоквартирных домов Приморского края» устанавливаются правила и процедуры контроля установки обновлений системного и прикладного программного обеспечения.

9.2. В программном обеспечении, поддерживающем автоматические обновления, таких как Java, Acrobat Reader и т. д. автоматические обновления не отключаются.

9.3. Общесистемное программное обеспечение и основное прикладное программное обеспечение обновляется во внерабочее время. Администратор перед обновлениями создает образы системы, точки восстановления и резервные копии баз данных.

9.4. Администратор контролирует источники обновлений программного обеспечения. Обновления должны осуществляться из доверенных источников, в соответствии с документацией на программное обеспечение.

9.5. Обновления общесистемного и основного прикладного программного обеспечения осуществляются не реже одного раза в неделю. Экстренные обновления осуществляются в случае поступления информации о критичных уязвимостях, для которых существует обновление безопасности.

9.6. Администратор в соответствии с эксплуатационной документацией на программное обеспечение осуществляет проверку установки обновлений, а также корректность установки обновлений. В ФПК «Фонд капитального ремонта многоквартирных домов Приморского края» должно применяться только такое программное обеспечение, которое поддерживает проверку целостности файлов обновлений.

9.7. Обновление антивирусных баз, сигнатур уязвимостей, баз решающих правил средств защиты информации осуществляется в соответствии с эксплуатационной документацией на СЗИ и разделами настоящей Политики.

9.8. Обновление микропрошивок и программного обеспечения BIOS/UEFI производится только при поступлении информации о критичных уязвимостях в таком программном обеспечении, применяемом в ФПК «Фонд капитального ремонта многоквартирных домов Приморского края».

## 10. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ СОСТАВА ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

10.1. Состав технических средств (далее – ТС), программного обеспечения и средств защиты информации (далее – СрЗИ) ИС фиксируется в техническом паспорте на информационную систему. Технический паспорт является эталоном состава ТС, ПО и СрЗИ, по которому осуществляется периодический контроль.

10.2. В случае добавления новых ТС, ПО и СрЗИ в состав ИС или удаления существующих компонентов, на основании акта ввода в эксплуатацию (или акта вывода из эксплуатации) максимально оперативно вносятся изменения в Технический паспорт.

10.3. Администратор осуществляет контроль состава ТС, ПО и СрЗИ не реже одного раза в месяц.

10.4. Регистрация событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты информации обеспечивается сертифицированным сканером безопасности

10.5. Выявление несоответствия состава ТС, ПО и СрЗИ техническому паспорту ИС является инцидентом безопасности. В случае выявления фактов несоответствия Администратор устанавливает причины самостоятельно или созывает ГРИИБ.

10.6. В случае выявления несоответствия состава ТС, ПО и СрЗИ, Администратор принимает меры по оперативному исключению (восстановлению) из состава (в составе) информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

10.7. Администратор осуществляет контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принимает меры, направленные на устранение выявленных недостатков. В случае, если сертификат соответствия истек, но был продлен производителем СрЗИ, Администратор запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СрЗИ, то Администратор сообщает об этом генеральному директору ФПК «Фонд капитального ремонта многоквартирных домов Приморского края», который принимает решение об организации самостоятельной сертификации использующегося СрЗИ, либо об обновлении использующегося СрЗИ до актуальной версии, либо о замене использующегося СрЗИ на другое аналогичное сертифицированное СрЗИ.

## 11. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

11.1. Администратор в СЗИ от НСД «Dallas Lock 8.0-K» настраивает контроль целостности (осуществляет расчет эталонных контрольных сумм) файлов и директорий прикладного программного обеспечения, операционных систем и средств защиты информации.

11.2. Нарушение целостности программного обеспечения является инцидентом информационной безопасности. В случае выявления таких инцидентов, Администратор принимает меры по их устранению самостоятельно или в составе ГРИИБ.

11.3. В ИС запрещено использование средств разработки и отладки программ.

## 12. ПРАВИЛА И ПРОЦЕДУРЫ РЕЗЕРВИРОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ, СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ИХ ВОССТАНОВЛЕНИЯ ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНЫХ СИТУАЦИЙ

12.1. Резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) ИС осуществляется в соответствии с инструкцией администратора безопасности информации и в соответствии с Приложением № 8 к настоящей Политике.

12.2. Администратор осуществляет с периодичностью, установленной в плане мероприятий по обеспечению режима защиты информации, проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий. По результатам проверки делается запись в журнале учета мероприятий по контролю за соблюдением режима защиты информации. В случае выявления проблем с системой резервирования, принимаются меры по восстановлению ее работоспособности. После восстановления работоспособности системы

резервирования осуществляется внеплановое резервное копирование всех информационных ресурсов ИС.

12.3. Резервирование технических средств осуществляется в соответствии с проектной документацией (эскизным проектом) на систему защиты информации ИС.

12.4. Восстановление из резервных копий является основным методом восстановления работоспособности информационной системы после ликвидации нештатных ситуаций.

12.5. Нештатными ситуациями являются:

- разглашение информации ограниченного доступа сотрудниками ФПК «Фонд капитального ремонта многоквартирных домов Приморского края», имеющими к ней право доступа, в том числе:
  - разглашение информации лицам, не имеющим права доступа к защищаемой информации;
  - передача информации по незащищенным каналам связи;
  - обработка информации на незащищенных технических средствах обработки информации;
  - опубликование информации в открытой печати и других средствах массовой информации;
  - передача носителя информации лицу, не имеющему права доступа к ней;
  - утрата носителя с информацией.
- неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:
  - несанкционированное изменение информации;
  - несанкционированное копирование информации;
- несанкционированный доступ к защищаемой информации:
  - несанкционированное подключение технических средств к средствам и системам ИС;
  - использование закладочных устройств;

- использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ИС;
- использование злоумышленником уязвимостей программного обеспечения ИС;
- использование злоумышленником программных закладок;
- заражение ИС злоумышленником программными вирусами;
- хищение носителей информации;
- нарушение функционирования технических средств обработки информации;
- блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;

- дефекты, сбои, отказы, аварии технических средств и систем ИС;
- дефекты, сбои, отказы программного обеспечения ИС;
- сбои, отказы и аварии систем обеспечения ИС;
- природные явления, стихийные бедствия:

- термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);
- механические факторы (повреждения зданий, землетрясения и т. д.);
- электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

12.6. В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей Политикой, Администратором, Ответственным и ГРИИБ вырабатывается конкретный план действий с учетом текущей ситуации.

12.7. Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении № 9 настоящей Политики.

12.8. С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации должны проводиться регулярные тренировки по различным видам нештатных ситуаций. В случае выявления, по результатам тренировок, изъянов в положениях настоящей Политики, касающихся реагирования на нештатные ситуации, в нее могут вноситься изменения.

12.9. Инциденты безопасности информации также являются нештатной ситуацией. При выявлении нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

12.10. В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:

– корректное отключение технических средств ИС до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;

– предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ИС, а также меры по замене/ремонту вышедших из строя средств и систем;

– в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.

12.11. В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями, выполняются следующие действия:

– Пользователи корректно отключают и обесточивают свои рабочие места;

– системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;

– Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;

– в случае нарушения корректной работы технических средств в ИС в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;

– в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации в результате стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;

– **в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.**

## 13. ПРАВИЛА ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ И ЗАЩИТЫ ОТ СПАМА

13.1. В настоящей Политике приведены только правила использования электронной почты, касающиеся вопросов информационной безопасности.

13.2. Администратор настраивает механизмы фильтрации спама на почтовом сервере.

13.3. Пользователи при работе с электронной почтой руководствуются положениями раздела 4 инструкции Пользователя.

13.4. Администратор настраивает блокирование потенциально опасных вложений в электронные письма на уровне почтового сервера. Блокировке подлежат, как минимум, следующие типы файлов: исполняемые файлы, файлы установщиков, файлы скриптов, файлы MS Office с макросами, архивы (в том числе и многотомные).

13.5. Администратор на уровне почтового сервера настраивает черные и белые списки адресатов и отправителей.

13.6. Пользователям информационных систем ФПК «Фонд капитального ремонта многоквартирных домов Приморского края», в том числе привилегированным, запрещено рассылать спам через почтовый сервер организации.

13.7. Администратор не реже одного раза в месяц проводит занятия с Пользователями на тему фишинговых писем, новых методов социальной инженерии и потенциально опасных вложений в электронных письмах.