АДМИНИСТРАЦИЯ
БУЙСКОГО МУНИЦИПАЛЬНОГО РАЙОНА
КОСТРОМСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 3 апреля 2019 года № 111

Об утверждении документов в области информационной безопасности в администрации Буйского муниципального района Костромской области

В соответствии с Федеральным законом от 06.10.2003 N 131-ФЗ "Об общих принципах администрации местного самоуправления в Российской Федерации", Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", руководствуясь Уставом муниципального образования Буйский муниципальный район Костромской области, в целях обеспечения информационной безопасности при использовании информационно-телекоммуникационной инфраструктуры, в том числе при использовании компьютерной сети «Интернет»,

администрация Буйского муниципального района ПОСТАНОВЛЯЕТ:

1. Утвердить документы в области информационной безопасности в администрации Буйского муниципального района Костромской области и ее структурных (функциональных) органов:

1) политику информационной безопасности в администрации Буйского муниципального района Костромской области и ее структурных (функциональных) органах (приложение № 1);

2) политику допустимого использования информационной системы в администрации Буйского муниципального района Костромской области и ее структурных (функциональных) органах (приложение № 2);

3) антивирусную политику в администрации Буйского муниципального района Костромской области и ее структурных (функциональных) органах (приложение № 3);

4) положение об использовании компьютерной сети «Интернет» в администрации Буйского муниципального района Костромской области и ее структурных (функциональных) органах (приложение № 4);

5) инструкцию по использованию электронной почты в администрации Буйского муниципального района Костромской области и ее структурных (функциональных) органах (приложение № 5);

6) правила использования системы Клиент-Банк в администрации Буйского муниципального района Костромской области и ее структурных (функциональных) органах (приложение № 6).

2. Старшему администратору отдела по общим вопросам администрации Буйского муниципального района (Т.С. Воронина) обеспечить доведение настоящего постановления до руководителей комитетов, управлений, отделов, секторов администрации Буйского муниципального района и должностных лиц, не входящих в их состав.

3. Руководителям управлений и комитетов администрации Буйского муниципального района ознакомить работников, находящихся в непосредственном подчинении с настоящим постановлением под роспись.

4. Возложить текущий контроль за исполнением настоящего постановления на системного администратора отдела по общим вопросам администрации Буйского муниципального района (Н.Б. Мовчан).

5. Возложить общий контроль исполнения настоящего постановления на управляющего делами-начальника отдела по общим вопросам администрации Буйского муниципального района (О.В. Смирнова).

6. Отделу по общим вопросам администрации Буйского муниципального района (Т.С. Воронина) обеспечить направление настоящего постановления для размещения на официальном сайте Буйского муниципального района Костромской области в сети «Интернет» в разделе персональные данные.

7. Настоящее постановление вступает в силу со дня его подписания.

Глава Буйского муниципального района А.М. Александров

Приложение № 1

УТВЕРЖДЕНО
постановлением администрации
Буйского муниципального района
Костромской области
от 03 апреля 2019 г. № 111

Политика
информационной безопасности в администрации Буйского муниципального района и ее структурных (функциональных) органах

1. ОБЩИЕ ПОЛОЖЕНИЯ

Политика информационной безопасности в администрации Буйского муниципального района и ее структурных (функциональных) органах (далее Политика) устанавливает порядок организации и правила обеспечения информационной безопасности в органах местного самоуправления Буйского муниципального района (далее по тексту – органах местного самоуправления Буйского муниципального района), распределение функций и ответственности за обеспечение информационной безопасности между подразделениями и сотрудниками, требования по информационной безопасности к используемым средствам информатизации.

Действие Политики распространяется на области деятельности органов местного самоуправления Буйского муниципального района, в которых для работы с информацией применяются различного рода технические средства.

Основные термины и определения:

– **администратор сети** – сотрудник администрации, отвечающий за поддержание работоспособности локальной вычислительной сети и разграничение доступа к информационным ресурсам этой сети;

– **безопасность информации** - состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования информации и т.п.;

– **доступ к информации** – комплекс организационно-технических мероприятий, позволяющих сотруднику получить возможность ознакомления с информацией, в том числе с помощью технических средств, в соответствии с предоставленными ему для этого правами;

– **защита информации** – комплекс организационно-технических мероприятий, направленных на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

– **защита информации от непреднамеренного воздействия** - деятельность, направленная на предотвращение воздействия на защищаемую

информацию ошибок её пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

– **защита информации от несанкционированного воздействия** – деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и(или) правил на изменение информации, приводящего к её искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

– **защита информации от несанкционированного доступа** – деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами и собственником прав или правил доступа к защищаемой информации;

– **информация** – сведения о лицах, предметах, событиях, явлениях и процессах (независимо от формы их представления), используемые в целях принятия решений;

– **информация** органов местного самоуправления Буйского муниципального района – информация, принадлежащая органам местного самоуправления Буйского муниципального района, то есть:

(а) созданная самими органами местного самоуправления Буйского муниципального района (его сотрудниками) в процессе его деятельности;

(б) приобретенная органами местного самоуправления Буйского муниципального района на законных основаниях;

(в) переданная органами местного самоуправления Буйского муниципального района его партнерами (клиентами) при установлении сотрудничества на правах совместного владения;

(г) полученная в результате целенаправленного сбора информации подразделениями органов местного самоуправления Буйского муниципального района;

– **информационная безопасность** – состояние защищённости информационной среды, обеспечивающее минимизацию ущерба, вызванного возможной утечкой защищаемой информации, а также несанкционированных и непреднамеренных воздействий;

– **информационная система** – организационно-упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием вычислительной техники;

– **информационная сфера (среда)** - совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений;

– **конфиденциальная информация** – документированная информация, включенная в Перечень сведений, составляющих коммерческую тайну предприятия, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

– **нарушение информационной безопасности** – факт

несанкционированного или непреднамеренного действия (операции) над информационной сферой, приводящий к нежелательным для предприятия последствиям;

– **несанкционированный доступ** – нарушение регламентированного доступа к объекту защиты;

– **обработка информации** – совокупность операций сбора, накопления, ввода, вывода, приёма, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией;

– **объект информатизации** - совокупность информационных ресурсов, средств и систем обрабртки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для конфиденциальных переговоров;

– **система защиты информации** – совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации;

– **средства связи** – технические средства, используемые для формирования, обработки, передачи или приёма сообщений электросвязи либо почтовых отправлений;

– **техническая защита информации** – защита (не криптографическими методами) информации, содержащей сведения, составляющие государственную или коммерческую тайну, от её утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию в целях её уничтожения, искажения и блокирования, и противодействие техническим средствам разведки;

– **угроза безопасности информации** - совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированным и/или непреднамеренным воздействиям на неё;

– **утечка информации** - неконтролируемое распространение защищаемой информации в результате её разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками;

– **шифрование** – способ защиты информации, заключающийся в криптографическом преобразовании информации по специальному алгоритму для получения шифротекста и позволяющий предотвратить ее несанкционированное использование;

– **цифровая подпись** – дополнительные данные или криптографическое преобразование какого-либо блока данных, позволяющие получателю блока данных убедиться в подлинности отправителя и целостности блока данных и защитить его от искажения с помощью, например, средств получателя.

Формы нарушения информационной безопасности:

а) пассивные

– получение информации нарушителем для использования в своих целях;

– анализ характеристик информации без доступа к самой информации;

б) активные

– изменение информации;
– внесение ложной информации
– нарушение (разрушение) информации;
– нарушение работоспособности системы обработки информации.

Принципы информационной безопасности:

– системный подход, предусматривающий комплексное решение проблемы информационной безопасности;

– ответственность всех сотрудников органов местного самоуправления Буйского муниципального района;

– непрерывность мер информационной безопасности;

– документальность любого действия в информационной системе для установления в последующем причины, авторства и самого факта совершения действия;

– компетентность в осуществлении мер информационной безопасности.

2. СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Состав системы

Общее руководство системой информационной безопасности и принятие всех решений по вопросам ее функционирования осуществляет **глава администрации Буйского муниципального района А. М. Александров**.

Исполнительные органы системы:

– администратор локальной вычислительной сети органов местного самоуправления Буйского муниципального района.

Организационные средства:

– настоящая Политика;
– отдельные руководящие документы на время их действия;
– протоколы информационных обследований;
– обязательства о неразглашении сведений, составляющих государственную тайну;
– журналы учета, установленные настоящей Инструкцией.

Технические средства:

– средства защиты от несанкционированного доступа к персональным компьютерам, программному обеспечению, сетям и информации;
– криптографические средства защиты компьютерной информации;
– средства защиты некомпьютерной информации.

2.2.1. Руководители функциональных (структурных) органов местного самоуправления Буйского муниципального района

Руководители функциональных (структурных) органов местного

самоуправления Буйского муниципального района несут персональную ответственность за организацию системы информационной безопасности в подчиненном подразделении и решают следующие задачи:

– осуществляют руководство работой по обеспечению информационной безопасности в функциональном (структурном) органе администрации ;

– организуют проведение первичного и контрольных информационных обследований функциональных (структурных), совместно с системным администратором, утверждают Актами результаты информационных обследований;

– после согласования главой администрации принимают решение о предоставлении прав доступа к информации функциональных (структурных) органов сотрудникам подчиненного подразделения и передают эти решения администратору сети для реализации;

– ходатайствуют перед руководителями других функциональных (структурных) органов о предоставлении прав доступа к информации этих подразделений сотрудникам подчиненного подразделения;

– готовят и направляют в отдел по защите информации заявки на установку специальных средств защиты информации, обучение сотрудников по вопросам информационной безопасности;

– взаимодействуют с отделом по защите информации по вопросам организации информационной безопасности.

2.2.2. Сотрудники функциональных (структурных) органов местного самоуправления Буйского муниципального района

Сотрудники функциональных (структурных) органов несут ответственность за соблюдение информационной безопасности на закрепленных участках работы. Сотрудники функциональных (структурных) органов:

– выполняют индивидуальные процедуры получения доступа к объектам информатизации и защищаемой информации;

– эксплуатируют пользовательские средства защиты информации, установленные на рабочих местах (если такие имеются);

– контролируют состояние информационной безопасности на своих рабочих местах.

2.2.3. Администратор сети

Функции администратора сети возлагаются на штатного сотрудника в обязанности которого входит администрирование локальной вычислительной сети органов местного самоуправления Буйского муниципального района. По вопросам обеспечения безопасности информации администратор сети подчиняется главе администрации. Администратор сети:

– составляет и ведет информационную схему сети;

– проводит совместно первичное и контрольные информационные обследования сети, подписывает протоколы и частные Акты обследований;

– эксплуатирует централизованные средства защиты информации в сети

(если такие есть);

– контролирует выполнение пользователями сети требований информационной безопасности и правильность эксплуатации пользовательских средств защиты информации (если такие есть), принимает меры к устранению недостатков и письменно сообщает о замеченных недостатках главе администрации или управляющему делами администрации;

– выполняет технологические операции по предоставлению прав доступа к ресурсам сети пользователям, которым эти права предоставлены решениями руководителей подразделений, согласованными с Управлением по защите информации;

– взаимодействует с управление цифрового развития администрации Костромской области

2.3. Информационное обследование

Информационное обследование включает в себя первичное обследование, проводящееся однократно при создании системы информационной безопасности, и контрольные обследования, проводящиеся по мере необходимости актуализации сведений об информационной системе.

Первичное информационное обследование имеет целью составление полной информационной схемы и категорирование информации, объектов информатизации, помещений и сотрудников подразделений органов местного самоуправления Буйского муниципального района.

Обследование состоит в полной проверке всех имеющихся рабочих мест на наличие на них информации, средств информатизации, программных продуктов и составления комплекта документов, содержащих спецификацию этих средств с точки зрения информационной безопасности и закрепляющих их текущее состояние.

Обследование проводится отдельно по функциональным (структурным) органам, а также в локальной вычислительной сети.

Мероприятия обследования функциональных (структурных) органов организует руководитель, а непосредственно проводят администраторы сети. Результатом обследования функциональных (структурных) органов являются документы:

1) Информационная схема функциональных (структурных) органов (исполняется руководителем) в составе:

– инвентарный план размещения средств информатизации и средств защиты информации функционального (структурного) органа с указанием их технических характеристик;

– перечень программных продуктов, установленных на каждом из средств информатизации или доступных с этого средства в сети и информации, обрабатываемой этими программными продуктами;

– список сотрудников функционального (структурного) органа с указанием закрепленных за ними средств информатизации и выделенных для них прав доступа;

2) Протоколы категорирования:

– информации;

– средств информатизации;

– помещений подразделения;

– сотрудников управления;

3) Протокол выявленных недостатков по обеспечению информационной безопасности с рекомендациями по ее совершенствованию;

4) Частный Акт информационного обследования функциональных (структурных) органов, закрепляющий текущее состояние информационной системы, описанное в Информационной схеме, подписываемый администратором сети и утверждаемый главой администрации;

5) План устранения недостатков и реализации рекомендаций информационного обследования.

Мероприятия обследования локальной вычислительной сети организует администратор сети. Результатом обследования сети являются документы:

1) Информационная схема локальной вычислительной сети (исполняется администратором сети) в составе:

– топологическая схема сети с указанием трасс прокладки кабелей, мест размещения серверов, сетевого оборудования и рабочих станций, привязанная к поэтажному плану здания;

– перечень программных продуктов, установленных в сети и информации, обрабатываемой этими программными продуктами;

– список пользователей сети с указанием выделенных им прав доступа;

2) Протокол категорирования программных продуктов и информации сети;

3) Протокол выявленных недостатков по обеспечению информационной безопасности с рекомендациями по ее совершенствованию;

4) Частный Акт информационного обследования локальной вычислительной сети, закрепляющий текущее состояние информационной системы, описанное в Информационной схеме, подписываемый администратором сети и сотрудником отдела по защите информации и утверждаемый начальником отдела по защите информации;

5) План устранения недостатков и реализации рекомендаций информационного обследования.

Контрольные информационные обследования проводятся по планам отдела по защите информации и вне планов – в случаях:

– реорганизации подразделений;

– крупных изменений в системе делопроизводства, составе оборудования и программного обеспечения;

– перемещений подразделений в другие помещения.

2.4. Категорирование

Категорирование – это специальная классификация различных объектов, имеющих отношение к информационной системе органов местного самоуправления Буйского муниципального района, по признаку конфиденциальности используемой информации и, соответственно, требуемого уровня ее защиты. В ходе категорирования все объекты разбиваются на группы (категории), для каждой из которых разрабатывается собственный уникальный комплекс мер защиты.

Категорированию подвергаются:

– используемая информация;

- средства;
- помещения;
- сотрудники функциональных (структурных) органов.

Категорирование производится в ходе первичного информационного обследования и уточняется при контрольных обследованиях. Настоящей Инструкцией вводятся следующие категории объектов информационной системы:

Категория	**Название**	Критерии
И н ф о р м а ц и я		
И-0	Коммерческая тайна	Недопустимы как активные, так и пассивные формы нарушения безопасности.
И-1	Служебная информация	Недопустимы систематические или крупномасштабные формы несанкционированного доступа.
И-2	Рабочая информация	**Несанкционированный доступ в любых формах неопасен.**
С р е д с т в а и н ф о р м а т и з а ц и и		
С-0	Средства особой важности	Недопустим несанкционированный доступ в любой форме, в том числе и физический доступ посторонних лиц.
С-1	Служебные средства	Допустим физический доступ посторонних лиц, однако использование без соответствующего уровня допуска исключается.
С-2	Рабочие средства	**Допустимо свободное использование вне зависимости от уровня допуска.**
П о м е щ е н и я		
П-0	Помещения особой важности	Доступ лиц, не имеющих соответствующих прав, запрещен.
П-1	Залы заседаний, комнаты переговоров	Допуск обеспечивается лицами, ответственными за организацию мероприятий.
П-2	Служебные помещения	Доступ посторонних лиц возможен только в сопровождении или при нахождении в помещении сотрудников подразделения, за которым помещение закреплено.
П-3	Рабочие помещения	Доступ не контролируется, меры по защите информации не требуются.
С о т р у д н и к и п о д р а з д е л е н и й		

Д-2	Должности с особыми полномочиями	Должности, предполагающие использование конфиденциальной, особо охраняемой информации.
Д-3	Должности основные	Должности с правами допуска к информации, ущерб от нарушения безопасности которой ограничен и поддается контролю.
Д-4	Должности вспомогательные	Должности с допуском к информации категорий не выше И-1
Д-5	Представители сторонних организаций	
Д-6	Представители государственных органов	
Д-7	Посетители	

2.5. Документирование

Основной формой документа в системе информационной безопасности является двусторонний Акт, который составляется и подписывается сотрудниками подразделения, в котором проводится мероприятие, с одной стороны, и сотрудниками Управления по защите информации с другой стороны. Акт утверждается начальником этого подразделения и начальником Управления по защите информации. К Акту прилагаются необходимые в каждом конкретном случае документы: протоколы, справки, схемы и т.д., исполненные в произвольной форме.

По решению главы администрации Буйского муниципального района акты могут докладываться для ознакомления и принятия решения руководителям органов местного самоуправления Буйского муниципального района.

В обязательном порядке составляются Акты в следующих случаях:

– при проведении первичного и контрольных информационных обследований;

– при проведении проверок состояния информационной безопасности отделом по защите информации;

– при предоставлении или изменении прав доступа к информации, средствам информатизации и сотрудникам;

– при выявлении нарушений информационной безопасности и их устранении.

2.6. Обучение персонала

Сотрудники органов местного самоуправления Буйского муниципального района (администраторы сети), непосредственно принимающие участие в обеспечении информационной безопасности, могут направляться на специальное обучение.

3. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Общие положения

Обеспечение информационной безопасности включает комплекс повседневно проводимых мероприятий, а именно:

– допуск (предоставление прав доступа) к информации, средствам информатизации и в помещения;

– доступ к информации, средствам информатизации и в помещения в соответствии с предоставленными правами;

– содержание средств информатизации;

– обеспечение безопасности информации;

– использование средств защиты информации;

– контроль состояния информационной безопасности;

– действия в случае выявления нарушений информационной безопасности;

– инструктаж по информационной безопасности.

3.2. Допуск

Допуск – это комплекс мероприятий, проводимых с целью предоставления прав доступа сотрудникам органов местного самоуправления Буйского муниципального района, представителям сторонних организаций и посетителям в помещения, к средствам информатизации и к информации органов местного самоуправления Буйского муниципального района.

Допуск заключается в предоставлении соответствующих прав доступа и документальном закреплении их за конкретным лицом, которому они предоставляются.

Право предоставления допуска имеет только руководитель функционального (структурного) органа, в ведении которого находятся объекты, к которым допускается указанное лицо. Руководитель функционального (структурного) органа полностью отвечает за соответствие уровня допуска задачам, решаемым допускаемым лицом. При этом должен строго соблюдаться принцип предоставления сотрудникам минимальных прав, достаточных для выполнения задач.

Допуск может предоставляться:

– сотрудникам своего функционального (структурного) органа;

– сотрудникам других функциональных (структурных) органов;

– сотрудникам сторонних организаций, выполняющим работы по заказу органаов местного самоуправления и их структурных (функциональных) органов с заключением контракта;

– сотрудникам государственных органов, имеющим соответствующие полномочия;

– посетителям.

Различаются постоянный и разовый допуск. Постоянный допуск предоставляется только сотрудникам органов местного самоуправления

Буйского муниципального района или представителям сторонних организаций, выполняющим работы по контракту. Разовый допуск предоставляется как сотрудникам органов местного самоуправления Буйского муниципального района, так и иным лицам, в том числе посетителям.

Порядок действий по предоставлению допуска зависит от того, к какому объекту допускается лицо, какова категория этого объекта, постоянный это допуск или разовый и кому он предоставляется: сотруднику своего подразделения, сотруднику другого подразделения, представителю сторонней организации или посетителю.

Допуск оформляется в письменной форме – для объектов категорий И-0, И-1, С-0, С-1, П-0, П-3 лицам, занимающим должности категорий Д-1…Д-3. Должностные лица категории Д-0 имеют допуск ко всей информации органов местного самоуправления Буйского муниципального района по положению. Лица категорий Д-5…Д-7 получают ограниченный допуск к отдельным массивам информации.

Допуск к объектам категорий И-2, С-2, П-4 обеспечивается устными распоряжениями руководителей подразделений.

Допуск к объектам категории П-1 предоставляется лицам всех категорий секретарями по указанию соответствующих руководителей.

Допуск к объектам категории П-2 может быть только разовым и осуществляется лицами, ответственными за организацию заседаний, совещаний и других мероприятий.

Постоянный допуск во всех случаях оформляется Актом, который составляется в функционального (структурного) органа в 2-х экземплярах, подписывается его сотрудниками, согласовывается с системным администратором. Допускается составление одного общего Акта сразу на нескольких сотрудников. В Акте для каждого сотрудника указываются подразделение, должность, фамилия, имя, отчество, перечень объектов, к которым предоставляется доступ, с указанием категории каждого объекта, цели доступа и предоставляемых прав, календарный период, на который предоставляется допуск. Первый экземпляр Акта хранится у системного администратора, второй экземпляр Акта хранится в подразделении.

Сотрудникам других структурных (функциональных) органов руководитель структурного (функционального) органа предоставляет постоянный допуск к подведомственным объектам на основании служебных записок от руководителей соответствующих структурных (функциональных) органов согласованных с системным администратором.

Максимальный срок постоянного допуска – 1 год, после чего он должен переоформляться.

Постоянный допуск сотрудникам сторонних организаций, выполняющим работы по контракту, предоставляется руководителем структурного (функционального) органа, ответственного за сопровождение контракта, после согласования с системным администратором при условии, что в контракте предусмотрены обязательства партнера по выполнению требований информационной безопасности и сохранению коммерческой тайны.

Разовый допуск предоставляется руководителем структурного (функционального) органа после согласования с системным администратором и оформляется письменно:

– сотрудникам своего подразделения – соответствующей записью в Журнале учета доступа за подписью руководителя подразделения;

– сотрудникам других подразделений – на основании служебной записки на имя начальника допускающего подразделения, соответствующей записью в Журнале учета доступа за подписью руководителя подразделения;

– сотрудникам сторонних организаций, выполняющих работы по контракту, - на основании служебной записки от подразделения, ответственного за проведение работ, на имя начальника допускающего подразделения, соответствующей записью в Журнале учета доступа за подписью руководителя подразделения;

– посетителям – соответствующей записью в Журнале учета доступа за подписью руководителя подразделения.

Не может быть предоставлен допуск:

– постоянный и разовый – сотрудникам сторонних организаций и посетителям к информации категории И-0 (посетителям – также и к информации категории И-1);

– постоянный и разовый – сотрудникам сторонних организаций и посетителям к средствам категорий С-0, С-1, если технически не исключена возможность их несанкционированного использования;

– постоянный – сотрудникам сторонних организаций в помещения категорий П-0, П-1, и П-2;

– постоянный и разовый – посетителям в помещения категорий П-0 и П-3;

– постоянный – посетителям в помещения категорий П-1, П-2.

Представителям органов местного самоуправления и государственных органов может быть предоставлен допуск к любым объектам информационной системы, но только разовый и в строгом соответствии с имеющимися у них полномочиями. Необходимость допуска письменно в обязательном порядке согласовывается с системным администратором.

Сотрудникам охраны (дежурных смен) предоставляется допуск во все помещения, категорированные по информационной безопасности, для выполнения ими обязанностей по обеспечению физической безопасности объектов.

3.3. Доступ

Доступ – это совокупность действий, выполняемых сотрудниками подразделений:

– с целью получения возможности использования информации в соответствии с имеющимся у них допуском;

– с целью предоставления возможности использования информации сотрудниками других подразделений, сторонних организаций, государственных органов и посетителями.

Таким образом, ***действия по доступу выполняются только сотрудниками допускающего подразделения***, даже если допускаются иные лица.

Порядок доступа в помещения категории П-0…П-2 определяется руководителем индивидуально. Учет доступа в помещения категории П-3 ведут

сотрудники охраны (ЧОП). Доступ в помещения категории П-4 не учитывается. Учет доступа к средствам информатизации и информации в локальной вычислительной сети ведет администратор сети.

Для учета доступа в отделе информационных технологий и в охране (ЧОП) заводятся Журналы учета доступа, в которых регистрируются факты получения доступа в зависимости от вида объекта информационной системы и его категории. Учету в Журнале доступа подлежат все факты предоставления доступа всем лицам, имеющим разовый допуск к информационным объектам категорий П-0, С-0, С-1, И-0, И-1.

Общая задача доступа подразделяется на подзадачи:

- доступ в помещения;
- доступ к средствам информатизации;
- доступ к программным продуктам и информации.

Действия по осуществлению доступа подразделяются на организационные и технические.

Ответственность за организацию доступа несет руководитель подразделения, а за правильное выполнение действий по доступу – сотрудник, их выполняющий.

3.3.1. Доступ в помещения

Доступ в помещения сотрудников, чьи рабочие места находятся в этих помещениях, осуществляется в соответствии с Инструкцией о пропускном режиме охраны (ЧОП) с учетом присвоенных этим помещениям категорий информационной безопасности.

Доступ в помещения сотрудников своего подразделения и сотрудников других подразделений, чьи рабочие места расположены в других помещениях, зависит от категории помещения:

– в помещения категории П-0 доступ возможен только при наличии соответствующего допуска через того из сотрудников, работающих в помещении, к которому этот посетитель прибыл;

– в помещения категории П-3 и П-4 доступ свободный.

Доступ в помещения сотрудников сторонних организаций и представителей государственных органов и органов местного самоуправления возможен только при наличии соответствующего допуска через того из сотрудников, работающих в помещении, к которому этот посетитель прибыл.

Доступ в помещения категории П-1 контролируется в рабочее время секретарями, в нерабочее время – сотрудниками охраны. Нахождение в этих помещениях кого бы то ни было, кроме владельцев кабинетов, секретарей и сотрудников охраны, без сопровождения секретарей (в рабочее время) или сотрудников охраны (в нерабочее время) строго запрещается.

Технические действия по доступу в помещения зависят от того, оборудованы ли помещения соответствующими техническими средствами и, как правило, состоят в снятии помещения с контроля системой охранной сигнализации и вскрытие помещения установленным порядком в начале рабочего дня.

Организационные действия по доступу в помещения выполняются сотрудниками, работающими в них, и заключаются в:

– проверке состояния помещения и находящихся в нем средств информатизации при вскрытии помещения и перед его закрытием;

– принятии мер по недопущению в помещения посторонних лиц, не имеющих допуска или нарушающих правила доступа;

– учете доступа в помещения в Журнале учета доступа там, где это необходимо.

Порядок доступа в помещения сотрудников охраны:

– в помещения категории П-0…П-3 – только в случаях прямой необходимости, в рабочее время - вместе с сотрудником, работающим в данном помещении, в нерабочее время - с последующим составлением служебной записки на имя Генерального директора ЧОП за подписью начальника смены с изложением причин доступа и описанием состояния помещения;

– в помещения категории П-4 – без ограничений.

3.3.2. Доступ к средствам информатизации

Доступ к средствам информатизации, находящимся на рабочих местах сотрудников (далее – «ответственные за средства информатизации»), осуществляется этими сотрудниками без ограничений.

Доступ к средствам информатизации сотрудников других подразделений, представителей сторонних организаций, представителей государственных органов, органов местного самоуправления и посетителей осуществляется в зависимости от категории:

– к средствам информатизации категорий С-0, С-1 – только при наличии допуска. При этом непосредственное использование средства информатизации осуществляется сотрудником, ответственным за него, а лицо, получившее доступ, присутствует при этом;

– к средствам информатизации категории С-2 – самостоятельно и без ограничений.

Для средств информатизации категорий С-0 и С-1 системным администратором должен быть заведен Аппаратный журнал, в котором отражаются все критичные операции и события (выход из строя, ремонт, техобслуживание и т.п.), а также операции по обеспечению информационной безопасности.

Управлению информационных систем и технологий ***категорически запрещёно подключение средств информатизации категорий С-0 и С-1 к ресурсам и сервисам международной компьютерной сети*** **Internet**.
Локальная вычислительная сеть, имеющая в своём составе средства информатизации категорий С-0 и С-1 не может иметь выход в международную сеть Internet.

Технические действия по осуществлению доступа заключаются в:

– включении питания;

– преодолении установленным порядком имеющихся средств защиты доступа (замок, вход по паролю, идентификация пользователя и др.).

Организационные действия заключаются в:

– ведении Аппаратного журнала;
– ведении Журнала учета доступа.

После того, как операции по доступу к средствам категорий С-0, С-1 выполнены, ответственный за средство информатизации обязан обеспечить невозможность использования средства кем-либо, кроме него самого. Запрещается даже на короткое время оставлять без контроля средство информатизации, если такая возможность не исключена технически.

Для доступа к средствам информатизации там, где это возможно, в обязательном порядке должен использоваться пароль, а доступ должен быть организован строго в соответствии с Руководством по применению паролей **(Приложение).**

3.3.3. Доступ к программным продуктам и информации

Порядок получения доступа к программным продуктам и информации определяется порядком доступа в помещения и к средствам информатизации. Ответственность за правильность доступа к программным продуктам и информации несут сотрудники, на рабочих местах которых используются эти программные средства и информация.

Доступ обеспечивается:

– к программным продуктам и компьютерной информации – имеющимися программно-аппаратными средствами защиты;

– к информации на бумажных носителях – принятой технологией несекретного «бумажного» делопроизводства;

– к речевой, видео- и другим видам информации – мерами обеспечения доступа в помещения и к средствам связи.

Технические действия по доступу к программным продуктам и информации заключаются в:

– запуске программного продукта;

– преодолении установленным порядком имеющихся программных и аппаратных средств защиты;

– регистрации доступа средствами регистрации, если они имеются.

Организационные действия по доступу к программным продуктам и информации заключаются в ведении Журнала учета доступа.

3.4. Содержание средств информатизации

Правильное с точки зрения информационной безопасности содержание (эксплуатация и хранение) средств информатизации предполагает:

– для средств информатизации категории С-0 – полное предотвращение доступа (в том числе и физического) к этим средствам любых лиц, не имеющих соответствующего допуска;

– для средств информатизации категории С-1 – предотвращение несанкционированного их использования;

– для средств информатизации категории С-2 – ограничений нет.

Содержание программных продуктов средств информатизации определяется содержанием технических средств информатизации (компьютеров, сетей), на которых эти программные продукты установлены.

Средства информатизации содержатся, как правило, на рабочих местах сотрудников, за которыми эти средства закреплены. Технические средства категории С-0 могут содержаться в кладовых или в сейфах.

В рабочее время ответственность за содержание средств информатизации несут сотрудники, за которыми эти средства закреплены, а в их отсутствие – их непосредственные начальники. В нерабочее время ответственность за хранение средств информатизации несет дежурная смена охраны.

Приемка в эксплуатацию средств информатизации (аппаратных, программных) категорий С-0 и С-1 проводится силами системных администраторов в следующем порядке:

– определяется категория средства информатизации;

– средство информатизации оснащается программными продуктами, устанавливается на рабочем месте и проверяется;

– производится проверка безопасности средства информатизации; при необходимости для такой проверки могут привлекаться специализированные организации;

– составляется и согласовывается с соответствующим подразделением перечень организационно-технических мероприятий, необходимых для обеспечения информационной безопасности средства информатизации, в том числе перечень средств защиты информации;

– средство информатизации, при необходимости, дополняется средствами защиты информации, из него исключаются не используемые «опасные» устройства и опечатывается;

– средство проверяется сотрудниками подразделения на предмет готовности к эксплуатации;

– составляется Акт о готовности средства информатизации по вопросам информационной безопасности, который утверждается начальниками отдела по защите информации и принимающего подразделения.

Каждое средство информатизации после приемки в эксплуатацию закрепляется письменным распоряжением руководителя подразделения за одним из сотрудников подразделения, который в дальнейшем отвечает за его содержание.

Сотрудник, ответственный за содержание средства информатизации, в части обеспечения информационной безопасности обязан:

– обеспечить установленный порядок доступа к средству информатизации;

– правильно использовать средства защиты информации, с которыми работает средство информатизации, если они имеются;

– при обнаружении признаков несанкционированного доступа к средству информатизации немедленно прекратить все работы с ним, обеспечить сохранение его в текущем состоянии и сообщить о случившемся своему руководителю и начальнику отдела по защите информации.

Учет средств информатизации ведется системным администратором в Журнале учета средств информатизации:

– технические средства информатизации учитываются в соответствии с их инвентарными номерами, которые присваиваются им при приемке в эксплуатацию;

– программные продукты средств информатизации учитываются поэкземплярно.

Дистрибутивы программных продуктов хранятся администратором сети таким образом, чтобы исключить возможность использования их для инсталляции несанкционированных копий программного продукта. Инсталляцию прикладных и автономных программных продуктов выполняет администратор сети.

Рабочие копии программных продуктов должны быть защищены от несанкционированной модификации программного кода и данных, для чего должны применяться различные методы, в том числе:

– установка программных продуктов на средствах информатизации соответствующей категории;

– установка программных продуктов на серверах сети с разделением доступа к ним, исходя из категорий пользователей;

– защита программных продуктов от копирования;

– шифрование исполняемых модулей и данных программных продуктов на носителях информации;

– запуск особо охраняемых программных продуктов категории С-0 и работа с информацией категории И-0 с гибких магнитных дисков, хранимых в сейфах.

Если доступ к средству информатизации защищается устройствами типа «замок» (механические замки, электронные замки, кодовые устройства и т.п.), имеющими «ключи» (обычные ключи, магнитные карты и т.п.), то оригинал ключа хранится у ответственного сотрудника, а дубликаты – у руководителя соответствующего подразделения. Хранение оригинала и дубликатов должно быть обеспечено таким образом, чтобы исключить возможность попадания ключа к кому-либо, кроме этих лиц. Все экземпляры ключей учитываются отдельными позициями в Журнале учета средств информатизации. В случае утраты ключа принимаются такие же меры, как при выявлении попытки несанкционированного доступа.

3.5. Обеспечение безопасности информации

Безопасность информации обеспечивается в соответствии с присвоенными ей категориями и предполагает:

– для информации категории И-0 – полное исключение возможности несанкционированного доступа к ней;

– для информации категории И-1 – исключение возможности несанкционированной модификации, предупреждение возможности анализа и статистической оценки;

– для информации категории И-2 – ограничений нет.

Основой безопасности информации является изложенная в п. 3.3. система контролируемого доступа в помещения, к средствам информатизации и самой информации. Кроме этого, в зависимости от формы представления информации,

с целью обеспечения ее безопасности принимаются специальные меры, изложенные ниже. Во всех случаях, за исключением специально оговоренных, ответственность за принятие этих мер несет сотрудник, использующий информацию или организующий мероприятие с ее использованием.

Безопасность информации в бумажной форме представления обеспечивается в соответствии с принятой технологией «бумажного» документооборота.

Для обеспечения безопасности речевой информации необходимо:

– ограничить число лиц, участвующих в переговорах, до минимально необходимого;

– проводить переговоры в местах, исключающих возможность подслушивания;

– применять специальные средства, если такие имеются.

Для обеспечения безопасности телефонных переговоров необходимо:

– безусловно исключить из обсуждения при ведении переговоров по открытым (незащищенным) телефонным линиям связи сведения, относящиеся к категории И-0 и ограничивать использование сведений категории И-1;

– применять специальные средства, если такие имеются.

Для обеспечения безопасности информации, обрабатываемой с помощью средств информатизации необходимо:

– обеспечить защиту от несанкционированного получения информации категории И-0 и защиту от модификации, а также возможность восстановления авторства доступа к информации категорий И-0, И-1, для чего в обязательном порядке применять все меры защиты, доступные на используемых программно-аппаратных средствах;

– обеспечить хранение носителей информации (дискет, магнито-оптических дисков, компакт-дисков и др.) с информацией категории И-0 способом, исключающим их утрату, несанкционированное копирование и получение;

– обеспечить хранение применяемых средств защиты информации, в том числе средств доступа к ним, способом, исключающим их несанкционированное использование.

3.6. Использование средств защиты информации

Средства защиты информации – это специальные технические средства, используемые для предупреждения несанкционированного использования всех видов информации. Разнообразие видов используемой информации, целей защиты, вариантов угроз, применяемых технологий защиты определяют широкую номенклатуру таких средств. В каждом случае необходимости защиты информации выбирается свой конкретный тип средства.

По вариантам использования различаются средства защиты информации:

– коллективные, применяемые для защиты информации, используемой одновременно несколькими (многими) сотрудниками;

– индивидуальные, применяемые только одним сотрудником для защиты информации, используемой им самим;

– сетевые, применяемые для защиты в вычислительных сетях и сетях

связи.

Необходимость применения средств защиты информации определяется при информационном обследовании, при принятии решения о применении информационной техники и в других случаях. Принятие решения на применение средств защиты, выбор способа защиты и типа средства защиты информации осуществляется совместно подразделением, которое использует защищаемую информацию, отделом по защите информации и утверждается главой администрации Буйского муниципального района. Выбор сетевых средств защиты осуществляют совместно отдел по защите информации и утверждает глава администрации Буйского муниципального района.

Решение о применении средств защиты информации в администрации или структурном (функциональном) органе администрации оформляется документом этого органа, согласуется системным администратором и представляется руководителем органа, защищающего свою информацию, для утверждения и выделения необходимых финансовых и технических средств главе администрации Буйского муниципального района

Закупку средств защиты информации производит отдел по экономическому развитию района администрации, совместно с системным администратором администрации.

Ответственность за использование средств защиты информации несут:

– за средства защиты коллективного пользования – специально назначаемые сотрудники;

– за средства защиты индивидуального пользования – сотрудники, на рабочих местах которых эти средства установлены;

– за сетевые средства защиты – администратор сети.

Закрепление средств защиты информации за ответственными за них сотрудниками производится письменным распоряжением руководителя соответствующего подразделения, первый экземпляр которого представляется и хранится в отделе по защите информации.

Порядок приемки в эксплуатацию средств защиты информации:

– средство устанавливается администратором сети на рабочем месте и проверяется в соответствии с инструкцией по эксплуатации;

– системный администратор и/или администратор сети производят совместную приемку средства с проверкой функционирования, разрабатывают организационные и технические меры по его эффективному использованию;

– сотрудник системный администратор и/ или администратор сети составляют и подписывают совместный Акт о приемке с приложением необходимых материалов и утверждают его у руководителя принимающего подразделения, после чего средство считается принятым в эксплуатацию;

– средство защиты информации передается в эксплуатацию назначенному ответственному сотруднику.

Сотрудник, ответственный за средство защиты информации, обязан:

– изучить средство в объеме, необходимом для правильной его эксплуатации;

– обеспечить установленный порядок использования средства: своевременно включать и выключать его, поддерживать эффективный режим работы;

– не допускать несанкционированного применения средства кем бы то ни было, обеспечить его сохранность, сообщать в отдел по защите информации обо всех попытках несанкционированного использования средства или подозрениях на такие попытки;

– проводить техническое обслуживание, обеспечивать его исправность, организовывать ремонт в случае выхода из строя и выполнять другие эксплуатационные операции.

Учет средств защиты информации ведется системным администратором администрации (функционального (структурного) органа в отдельном разделе Журнала учета средств информатизации в соответствии с их инвентарными номерами, которые присваиваются им при приемке в эксплуатацию.

3.7. Контроль состояния информационной безопасности

Контроль состояния информационной безопасности проводится с целью проверки ее организации, а также предупреждения и своевременного выявления случаев ее нарушения.

Обязанности по контролю распределяются между исполнительными органами системы информационной безопасности следующим образом:

– Системный администратор проводит проверки организации и состояния информационной безопасности;

– сотрудники контролируют текущее состояние информационной безопасности на своих рабочих местах;

– администратор сети повседневно контролирует текущее состояние информационной безопасности в локальной вычислительной сети;

– руководители подразделений повседневно контролируют текущее состояние информационной безопасности в своих подразделениях;

– сотрудники контролируют текущее состояние информационной безопасности на своих рабочих местах.

Проверки организации и состояния информационной безопасности проводятся системными администратора администрации (функциональных (структурных) органов ее) и в сетях и могут быть:

– плановыми;
– внезапными;
– по фактам нарушения информационной безопасности.

Плановые проверки проводятся в соответствии с годовым Планом проверок, который составляется на очередной год в декабре текущего года, подписывается руководителями подразделений и утверждается главой администрации Буйского муниципального района. В ходе плановых проверок должна полностью проверяться вся организация системы информационной безопасности.

Внезапные проверки проводятся системным администратором в соответствии с внутренними планами работы. Внезапные проверки проводятся по отдельным вопросам организации информационной безопасности.

Проверки по фактам нарушения информационной безопасности проводятся отделом по защите информации после того, как нарушение устранено.

Проверка проводится с целью выявления причин и предпосылок нарушения и выработки мер по предупреждению подобных нарушений в дальнейшем. Проверка проводится в обязательном порядке по каждому факту нарушения независимо от его последствий.

Результаты всех проверок оформляются двусторонними Актами между проверяющей и проверяемой сторонами, с необходимыми в каждом конкретном случае приложениями и утверждаются главой администрации Буйского муниципального района. При возникновении разногласий с проверяемым подразделением может оформляться односторонний Акт отделом по защите информации.

Для текущего контроля состояния информационной безопасности независимо от работы информационной системы и сотрудников органов местного самоуправления Буйского муниципального района, системными администраторами должны применяться специальные средства, такие как специальное автоматизированное рабочее место (АРМ безопасности), различные технические средства для оценки эффективности применяемых методов и средств обеспечения безопасности.

Администратор сети контролирует состояние информационной безопасности на подведомственных участках:

– контролирует выполнение сотрудниками установленного порядка действий по доступу к объектам информационной системы;

– анализирует состояние информационной системы с целью выявления попыток несанкционированного доступа и использования средств информатизации и информации;

– контролирует правильность использования имеющихся коллективных и индивидуальных средств информационной защиты.

В случае выявления каких-либо отклонений или нарушений в системе информационной безопасности администратор сети немедленно обязан принять все меры к их устранению самостоятельно, через руководителя соответствующего подразделения или с привлечением Управления по защите информации. Ответственность за принятие этих мер и сообщение о происшедшем руководителю подразделения и в отдел по защите информации несет администратор сети.

Сотрудники подразделений анализируют состояние своих рабочих мест с целью выявления попыток несанкционированного доступа и использования средств информатизации и информации. В случае выявления таких попыток сотрудник немедленно обязан сообщить об этом администратору сети и своему руководителю.

3.8. Порядок действий в случае выявления нарушений информационной безопасности

Действия, предпринимаемые в случае выявления нарушений информационной безопасности, состоят в следующем:

– выявление факта нарушения;

– прекращение всех операций, связанных с участком, на котором произошло нарушение;

– принятие экстренных мер для прекращения несанкционированного доступа или использования информации;

– оповещение о нарушении;

– восстановление работоспособности информационной системы;

– расследование причин нарушения информационной безопасности;

– проверка состояния информационной безопасности по факту нарушения.

Выявление факта нарушения, как правило, происходит в ходе контроля состояния информационной безопасности сотрудником подразделения, администратором сети или сотрудниками отдела по защите информации.

Немедленно после выявления нарушения сотрудник, который обнаружил его, обязан прекратить все операции по использованию по назначению информации и средств информатизации, которые выполнялись на участке, где произошло нарушение, а также, если необходимо, на смежных участках. Если выявлен несанкционированный доступ в категорированные помещения, всякий доступ в него должен быть прекращен.

Если на момент выявления нарушения несанкционированный доступ или использование средств информатизации и информации еще продолжаются, сотрудник, выявивший их, обязан немедленно принять меры к их прекращению. Конкретное содержание этих мер зависит от того, каков характер нарушения, то есть информационный объект какой категории попал под нарушение, какой ущерб может быть нанесен нарушением, какие побочные последствия повлечет принятие этих мер. По возможности следует привлечь для выработки и принятия мер администратора сети, руководителя подразделения, сотрудников отдела по защите информации. Ответственность за адекватность принимаемых мер несут в порядке привлечения сотрудник, выявивший нарушение, администратор сети и руководитель подразделения.

После того, как нарушение выявлено и блокировано, производится срочное оповещение о нем в следующем порядке:

– сотрудник оповещает руководителя своего подразделения, системного администратора и/или администратора сети;

– руководитель подразделения оповещает других сотрудников своего подразделения на участках ответственности которых могут возникнуть подобные нарушения;

– системный администратор оповещает другие подразделения, на участках ответственности которых могут возникнуть подобные нарушения.

С целью минимизации ущерба от прекращения работы информационной системы немедленно после того, как возможность дальнейшего нарушения информационной безопасности устранена, принимаются меры для восстановления ее работы. Решение на восстановление работы принимает руководитель подразделения, на участке ответственности которого произошло

нарушение, по согласованию с системным администратором и/ или администратором сети.

Расследование причин нарушения производится системным адмимнистратором, при этом все связанные с нарушением сотрудники должны оказывать содействие расследованию. Целью расследования является выявление истинных причин нарушения и предпосылок к нему для принятия мер к недопущению его повторения. Расследование проводится сразу после восстановления работоспособности информационной системы, в обязательном порядке, независимо от последствий, которые повлекло нарушение. Результаты расследования оформляются двусторонним Актом системного администратора, подразделения, в котором произошло нарушение и утверждаются главой администрации Буйского муниципального района.

По факту нарушения проводится также проверка системы информационной безопасности на тех ее участках, где подобные нарушения возможны.

3.9. Инструктаж

Для обучения сотрудников и иных лиц, имеющих допуск к информации органов местного самоуправления Буйского муниципального района, правилам обеспечения информационной безопасности и поддержания их знаний и навыков в соответствии с текущей обстановкой на рабочих местах организуется их инструктаж. Проводятся следующие виды инструктажа:

- вводный;
- периодический;
- разовый.

Инструктаж проводит системный администратор.

Кроме этих видов инструктажа, при допуске сотрудника и иных лиц в качестве пользователя сети администратор сети проводит с ним вводный инструктаж.

При вводном инструктаже сообщаются сведения:

- категория должности, занимаемой сотрудником;
- перечень средств информатизации и программных продуктов, имеющихся на его рабочем месте и смежных рабочих местах, их категории;
- перечень помещений, в которые он имеет допуск, их категории;
- перечень информации, к которой он имеет допуск, и его права доступа к ней;
- порядок доступа и работы с каждым из названных объектов в соответствии с его категорией, при необходимости содержание Руководства по применению паролей;
- порядок содержания средств информатизации;
- порядок обеспечения безопасности информации;
- порядок использования средств защиты информации, если они имеются;
- обязанности сотрудника по контролю за информационной безопасностью;
- возможные варианты нарушений информационной безопасности на

конкретном рабочем месте;

– действия при выявлении нарушений информационной безопасности.

Периодический инструктаж проводится один раз в год. В периодический инструктаж включается краткое изложение вопросов вводного инструктажа и подробное – изменений по этим вопросам, произошедшим со времени предыдущего инструктажа.

Разовый инструктаж проводится при проведении отдельных мероприятий по обеспечению информационной безопасности.

Инструктаж пользователя сети, проводимый администратором сети, включает:

– перечень программных продуктов, сетевых устройств, разделов памяти сетевых устройств и информации, к которым пользователь имеет доступ в сети, права доступа пользователя и категории этих объектов информационной системы;

– порядок доступа в сеть, в том числе содержание Руководства по применению паролей;

– порядок использования средств защиты информации в сети, если они имеются;

– особенности контроля за информационной безопасностью, варианты ее нарушений, действия при выявлении нарушений, если эти действия носят какие-либо особенности относительно общепринятых.

Инструктаж во всех случаях оформляется соответствующей записью в Журнале инструктажа по информационной безопасности, который заводится для этих целей в отдел по защите информации, и заверяется росписью инструктируемого сотрудника и лица, проводившего инструктаж.

Приложение № 2

УТВЕРЖДЕНО
постановлением администрации
Буйского муниципального района
Костромской области
от 3 апреля 2019 г. № 111

Политика
допустимого использования информационной системы в администрации Буйского муниципального района Костромской области

1. Обзор

Политика допустимого использования информационной системы не направлена на навязывание ограничений, идущих вразрез с текущей политикой администрации Буйского муниципального района Костромской области. Напротив, её целью является создание культуры доверия и целостности. администрация Буйского муниципального района Костромской области стремится защищать своих сотрудников, партнёров и бизнес от незаконных или опасных действий, неважно, осознанных или нет.

Системы, работающие в интернет/интранет/экстранет, включая, но не ограничиваясь компьютерным оборудованием, программным обеспечением, операционными системами, устройствами хранения данных, сетевыми учётными записями, обеспечивающими доступ к электронной почте, веб-ресурсам, ftp-серверам, являются собственностью администрации Буйского муниципального района Костромской области. Эти системы используются в повседневной деятельности в интересах компании, клиентов, потребителей и стабильной работы поставщиков. Более полная информация находится в Правилах трудового распорядка.

Обеспечение безопасности это совместная работа и участие каждого сотрудника и подразделения администрации Буйского муниципального района Костромской области, которые работают с информацией и/или информационными системами. Сотрудники администрации как пользователь информационной системы, должны знать и следовать этим рекомендациям.

2. Назначение

Настоящая политика описывает допустимое использование компьютерного оборудования в информационной системе администрации Буйского муниципального района Костромской области. Правила защищают сотрудников и администрацию Буйского муниципального района Костромской области. Ненадлежащее использование информационной системы подвергает администрацию Буйского муниципального района Костромской области риску, включая вирусные атаки, взлом компьютерных сетей и нарушение работы администрации.

3. Аудитория

Политика распространяется на постоянных сотрудников, контрактных работников, консультантов, временно трудоустроенных и других работников, включая третью сторону. Политика распространяется на всё оборудование, которое является собственностью или арендовано администрацией Буйского муниципального района Костромской области.

4. Политика

4.1. Общие правила и ответственность

4.1.1. В связи с тем, что администрация Буйского муниципального района Костромской области стремится обеспечить разумный уровень защиты информации, все данные, созданные внутри корпоративной системы, являются ее собственностью. Для обеспечения безопасности информационной системы администрации Буйского муниципального района Костромской области, руководство гарантирует конфиденциальность информации, размещённой на любом сетевом ресурсе администрации Буйского муниципального района Костромской области».

4.1.2. Каждый отдел должен руководствоваться правилами в отношении использования интернет/интранет/экстранет ресурсов. При отсутствии урегулирования каких-либо вопросов в Правилах, необходимо следовать общей политике, и в случае неясностей проконсультироваться у своего руководителя.

4.1.3. Рекомендуется шифровать информацию, отнесенную к категории секретной или уязвимой. Правила классификации информации находятся в политике секретности информации.

4.1.4. В целях обеспечения безопасности и поддержания работоспособности информационной системы, системный администратор отдела по общим вопросам администрации Буйского муниципального района Костромской области может наблюдать за оборудованием, системами и сетевой активностью в любое время в соответствие с Политикой аудита.

4.1.5. Администрация Буйского муниципального района Костромской области оставляет за собой право производить периодический аудит информационной системы с целью обеспечения выполнения требований настоящей политики.

4.2. Безопасность и внутренняя информация

4.2.1. Пользовательский интерфейс для работы с информацией, содержащейся в интернет/интранет/экстранет-системах должен рассматриваться как конфиденциальный или не конфиденциальный в соответствие с правилами служебной безопасности Правил трудового распорядка. Примерами конфиденциальной информации являются: частные данные администрации, корпоративная стратегия, спецификации, перечень контрагентов по договорам, персональные данные сотрудников администрации и граждан, сведения составляющие государственную тайну. Вам необходимо предпринять все необходимые действия для предотвращения неавторизованного доступа к этой информации.

4.2.2. Сотрудники администрации обязаны держать пароли в тайне и не позволять использовать свои учётные данные. Будучи зарегистрированным

пользователем, сотрудники ответственные за свои пароли и учётные записи, и обязаны менять пароли доступа в систему ежеквартально, менять пароль пользователя каждые полгода.

4.2.3. Сотрудники администрации обязаны защищать компьютеры, ноутбуки и рабочие станции скринсейвером с автоматической активацией парольной защиты в течение 10 минут или менее или блокировать систему (Ctrl-Alt-Delete, Блокировка) при уходите с рабочего места.

4.2.4. Сотрудники администрации обязаны использовать шифрование информации в соответствие Политикой шифрования.

4.2.5. Так как информация на переносных компьютерах крайне уязвима, Сотрудники администрации обязаны уделять им особое внимание, защищать ноутбуки в соответствие с Рекомендациями по защите ноутбуков.

4.2.6. Сообщения в форумах, содержащие адрес корпоративной электронной почты должны содержать уведомление, что высказывания основаны на личном мнении сотрудника и могут не разделяться администрацией Буйского муниципального района Костромской области, за исключением случаев когда сообщения размещаются в связи с профессиональной деятельностью сотрудника.

4.2.7. Все используемые сотрудниками компьютеры, имеющие доступ к интернет/интранет/экстранет системам, принадлежащие сотрудникам или администрации Буйского муниципального района Костромской области, должны использовать антивирусное ПО с актуальными антивирусными базами (кроме иных случаев, определённых групповой политикой или политикой отдела).

4.2.8. Сотрудники администрации обязаны использовать все меры предосторожности при открытии вложений в письмах от неизвестных отправителей. Эти вложения могут содержать вирусы, почтовые бомбы или троянских коней.

4.3. Недопустимое использование

4.3.1.Следующая деятельность в большинстве случаев запрещена. В особых случаях Сотрудники администрации обязаны могут не подпадать под эти ограничения во время исполнения своих трудовых обязанностей (например, системный администратор может отключить доступ в сеть компьютера, который нарушает работу сети).

4.3.2.Ни при каких обстоятельствах сотрудник, используя ресурсы администрации Буйского муниципального района Костромской области, не может заниматься деятельностью, которая является незаконной по местному, федеральному или международному законодательству.

4.3.3. Список ни в коей мере не является полным, он представляет собой часть видов деятельности, которые подпадают в категорию «недопустимого использования».

4.4. Работа в системах и сети. Следующая деятельность запрещается без каких-либо исключений:

4.4.1. Нарушение прав любого лица или компании, защищённых авторскими правами, коммерческой тайной, патентом или другой интеллектуальной собственности на основе соответствующих законов, включая, но не ограничиваясь установкой «пиратского» или другого программного обеспечения, которое не лицензировано для использования в администрации Буйского муниципального района Костромской области.

4.4.2. Неавторизованное копирование материалов, защищённых авторским правом, включая, но, не ограничиваясь оцифровыванием и распространением фотографий из журналов, книг или других источников, защищённых авторским правом, музыки, защищённой авторским правом и установкой программного обеспечения, защищённого авторским правом, на которое у администрации Буйского муниципального района Костромской области или конечного пользователя отсутствует активная лицензия.

4.4.3. Экспорт программного обеспечения, технической информации, криптопрограмм или криптотехнологий в нарушение международных или внутренних экспортных законов.

4.4.4. Размещение вредоносных программ в сети или на сервере (например, вирусов, червей, троянских коней, почтовых бомб и т. д.).

4.4.5. Сообщение пароля от вашей учётной записи или использование вашей учётной записи посторонним. К посторонним относятся члены семьи и другие лица при работе дома.

4.4.6. Использование оборудования администрации Буйского муниципального района Костромской области для добычи или распространения материалов, нарушающих законодательство.

4.4.7. Размещение мошеннических предложений товаров или услуг с использованием учётной записи администрации Буйского муниципального района Костромской области.

4.4.8. Заявления о гарантиях, явных или подразумеваемых, кроме случаев, когда это входит в трудовые обязанности.

4.4.9. Создание уязвимостей или прерывание работы сети. Уязвимости включают, но не ограничиваются доступом к данным, получателем которых сотрудник не является или входом на сервер или ресурс, доступ к которому сотруднику явно не предоставлен, кроме случаев, когда эта деятельность является частью ваших прямых обязанностей. «Прерывания» включают в себя, но не ограничиваются перехватом пакетов, пинговой атакой, подменой пакетов, отказом от обслуживания и поддельными данными маршрутизации для злонамеренных действий.

4.4.10. Сканирование портов или обнаружение уязвимостей без предварительного уведомления системного администратора отдела по общим вопросам администрации Буйского муниципального района Костромской области.

4.4.11. Любой вид сетевого мониторинга, при котором перехватываются данные, не адресованные вашему узлу, кроме случаев, когда это является частью вашей трудовой деятельности.

4.4.12. Обход систем входа и безопасности любого узла, сети или учётной записи.

4.4.13. Намеренное прекращение работы пользователей информационной системы (например, DOS-атака).

4.4.14. Использование любой программы/скрипта/команды, или рассылка любых сообщений с целью отключения терминальной сессии пользователя.

4.4.15. Предоставление информации или перечня сотрудников лицам за пределами администрации Буйского муниципального района Костромской области.

Приложение № 3

УТВЕРЖДЕНО
постановлением администрации
Буйского муниципального района
Костромской области
от 3 апреля 2019 г. № 111

Антивирусная политика
в администрации Буйского муниципального района Костромской области

Настоящая политика определяет требования по защите информационно-телекоммуникационной инфраструктуры администрации Буйского муниципального района Костромской области от угроз информационной безопасности, причина возникновения которых связанна с распространением вредоносного программного обеспечения. Данные требования минимизируют вероятность возникновения негативных последствий для ИТКИ администрации Буйского муниципального района Костромской области вследствие отсутствия защиты информационно-телекоммуникационной инфраструктуры. Негативные последствия могут включать в себя раскрытие или утрату чувствительной и конфиденциальной информации, кражу интеллектуальной собственности, репутационные последствия, а также влияние на важные внутренние системы администрации Буйского муниципального района Костромской области.

1. Необходимо использовать только полученное из доверенного источника и принятое в качестве стандарта в администрации Буйского муниципального района Костромской области антивирусное программное обеспечение.

Системный администратор отдела по общим вопросам администрации поддерживает антивирусное программное обеспечение в актуальном состоянии.

2. Сотрудники администрации обязаны не открывать вложения к сообщениям электронной почты, полученным из неизвестных, подозрительных или недостоверных источников. Такие вложения должны незамедлительно удаляться.

3. Сообщения электронной почты содержащей спам, цепочки сообщений и другую нежелательную почту должны удаляться без пересылки, в соответствии с принятой в администрации Буйского муниципального района Костромской области Политикой допустимого использования ИС.

4. Сотрудники администрации обязаны не скачивать информацию из неизвестных или подозрительных источников.

5. Необходимо избегайть предоставления общего доступа к логическим дискам с правами чтения/записи, в случае если это не требуется в рамках выполнения основной деятельности.

6. Прежде чем использовать носители информации, полученные от неизвестных или подозрительных источников, сотрудники обязаны сканировать их на отсутствие вирусов.

7. Резервируйте важные данные и настройки системы регулярно. Резервные копии храните в безопасном месте.

8. В случае необходимости запуска приложения, конфликтующего с установленным антивирусным программным обеспечением, необходимо выполнить полную проверку рабочей станции на наличие вирусов, отключить антивирусное программное обеспечение и запустить необходимое приложение. Должно быть доподлинно известно, что запускаемое приложение не приведет к негативным последствиям. После выполнения задач связанных с использованием приложения, возобновите работу антивирусного программного обеспечения. При отключенном антивирусном программном обеспечении запрещается запускать любые приложения (электронная почта или открытие общего доступа к файловым ресурсам) в результате действия которых ваша рабочая станция может быть подвержена инфицированию вредоносным программным обеспечением.

9. Появление нового вредоносного программного обеспечения обнаруживаются ежедневно.

Приложение № 4

УТВЕРЖДЕНО
постановлением администрации
Буйского муниципального района
Костромской области
от 3 апреля 2019 г. № 111

Положение
об использовании компьютерной сети «Интернет» в администрации Буйского муниципального района Костромской области

1. Общие положения

1.1. Настоящее Положение устанавливает порядок использования сети Интернет работниками администрации Буйского муниципального района Костромской области (далее - администрация).

1.2. Действие настоящего Положения распространяется на работников администрации, подрядчиков и третью сторону, работающую на территории администрации.

2.Основные термины, сокращения и определения

- Администратор ИС – системный администратор, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО.
- Адрес IP – уникальный идентификатор АРМ, подключенного к ИС Администрации, а также сети Интернет.
- АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной задачи.
- Интернет – глобальная ИС, обеспечивающая удаленный доступ к ресурсам различного содержания и направленности.
- ИБ – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.
- ИС – информационная система Администрации – система, обеспечивающая хранение, обработку, преобразование и передачу информации Администрации с использованием компьютерной и другой техники.
- ИТ – информационные технологии – совокупность методов и процессов, обеспечивающих хранение, обработку, преобразование и передачу информации Администрации с использованием средств компьютерной и другой техники.
- Паспорт ПК – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.
- ПК – персональный компьютер.
- ПО – программное обеспечение вычислительной техники, базы данных.
- ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.
- ПО коммерческое – ПО сторонних производителей

(правообладателей). Предоставляется в пользование на возмездной (платной) основе.

- Пользователь – работник администрации, использующий ресурсы Интернет для выполнения своих должностных обязанностей.
- Администрация – администрация Буйского муниципального района Костромской области.
- Третья сторона – лицо или администрация, считающаяся независимой по отношению к администрации.

3. Порядок использования сети Интернет

3.1. Доступ к сети Интернет предоставляется определенному кругу работников администрации в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

3.2. Для доступа работников администрации к сети Интернет допускается применение коммерческого ПО.

3.3. Операции по предоставлению доступа работников администрации к сети Интернет и контролю его использования выполняются непосредственно (при участии) администраторами ИС.

3.4. Доступ работнику Администрации к сети Интернет может быть инициирован Руководителем структурного подразделения в случаях:

- необходимости администрации АРМ для нового работника;
- необходимости выполнения работника новых (дополнительных) обязанностей, для которых требуется доступ к внешним ресурсам.

3.5. Подключение АРМ работника выполняется на месте специалистами отдела ИТ.

3.6. АРМы, используемые для обработки критичной информации, не могут быть подключены к сети Интернет.

3.7. При использовании сети Интернет необходимо:

3.7.1. Соблюдать требования настоящего Положения.

3.7.2. Использовать сеть Интернет исключительно для выполнения своих служебных обязанностей.

3.7.3. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Положения.

3.8. При использовании сети Интернет запрещено:

3.8.1. Использовать предоставленный организацией доступ в сеть Интернет в личных целях.

3.8.2. Использовать специализированные аппаратные и программные средства, позволяющие работникам администрации получить несанкционированный доступ к сети Интернет.

3.8.3. Совершать любые действия, направленные на нарушение нормального функционирования элементов ИС администрации.

3.8.4. Публиковать, загружать и распространять материалы содержащие:

3.8.4.1. Конфиденциальную информацию, а также информацию, составляющую государственную тайну, за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с администраторами ИС заранее.

3.8.4.2. Информацию, полностью или частично, защищенную авторскими или другим правами, без разрешения владельца.

3.8.4.3. Вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера к коммерческому ПО и ПО для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным Интернет-ресурсам, а также ссылки на вышеуказанную информацию.

3.8.4.4. Угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и т.д.

3.8.5. Фальсифицировать свой IP-адрес, а также прочую служебную информацию.

3.9. Администрация оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством.

3.10. Блокирование и ограничение доступа пользователей к Интернет-ресурсам осуществляется на основе Регламента применения категорий Интернет-ресурсов.

3.11. Информация о посещаемых работниками администрации Интернет-ресурсах протоколируется для последующего анализа и, при необходимости, может быть предоставлена руководителям структурных подразделений, а также главеу администрации для контроля.

3.12. При подозрении работника администрации в нецелевом использовании сети Интернет инициализируется служебная проверка, проводимая комиссией, состав которой определяется главой администрации.

3.13. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам администрации и действующему законодательству. Акт расследования инцидента и сведения о принятых мерах подлежат передаче в отдел по общим вопросам.

3.14. Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

4. Ответственность за нарушение настоящих Правил

4.1. Работники, нарушившие требования настоящего Положения по решению главы администрации или структурного органа администрации, в чьем непосредственном подчинении находится допустивший нарушения сотрудник могут быть привлечены к дисциплинарной ответственности, если иная ответственность не предусмотрена Федеральным законодательством.

5. Внесение изменений и дополнений

5.1. Изменения и дополнения в настоящее Положение вносятся работниками отдела по общим вопросам (Системным администратором или Управляющим делами администрации) по указанию начальника отдела, и после согласования с руководителями администрации утверждаются распоряжением администрации.

5.2. Все изменения и дополнения настоящего Положения вступают в силу с момента их утверждения.

Приложение № 5

УТВЕРЖДЕНО
постановлением администрации
Буйского муниципального района
Костромской области
от 3 апреля 2019 г. № 111

Инструкция
по использованию электронной почты в администрации Буйского муниципального района Костромской области

1. Электронная почта предоставляется работникам администрации только для исполнения своих служебных обязанностей. Использование ее в личных целях запрещено.

2. Размер почтового ящика пользователя ограничен «10» Гб. В случае превышения указанного лимита прием корреспонденции для пользователя прекращается до момента появления свободного места в почтовом ящике.

3. Электронная почта используется для обмена служебной информацией в виде текстовых сообщений или документов в электронном виде.

4. Действуют следующие правила для блокирования исходящей корреспонденции: блокируются исходящие и входящие электронные сообщения следующего вида:

- сообщения без темы;
- сообщения, одновременно адресованные более 25 корреспондентам;
- сообщения, содержащие вложенные файлы следующих форматов:
- исполняемые файлы (расширения – .exe, .dll, .pif и т.п.);
- мультимедиа файлы (аудио и видео);
- сообщения, содержащие более «10» вложенных файлов;
- сообщения размером свыше «30» Мб.

5. Для уменьшения размера электронных сообщений и объединения нескольких вложенных файлов в один рекомендуется использовать программы для сжатия (компрессии) вложенных документов (Win Rar).

Пользователям ЗАПРЕЩАЕТСЯ:

- использовать корпоративную электронную почту в личных целях;
- производить рассылку материалов рекламного (непрофильного) и развлекательного характера;
- производить массовую рассылку писем не служебного характера, кроме;
- пересылать исполняемые файлы (с расширениями – .exe, .dll, .pif и т.п.);
- пересылать мультимедийные файлы (аудио и видео) не служебного характера;
- производить рассылку вредоносных программ или файлов, зараженных вирусами;
- использовать электронную почту для передачи материалов

большого объема (более «30» Мб);

- публиковать свой корпоративный адрес, либо адреса других работников компании на общедоступных Интернет ресурсах (форумы, конференции и т.п.);
- осуществлять массовую рассылку почтовых сообщений рекламного характера без предварительного согласования с сотрудниками общего отдела, в частности с системным администратором;
- предоставлять, кому бы-то ни было пароль доступа к своему почтовому ящику;
- пересылать по эл. почте пароли к каким бы то ни было ресурсам Администрации.

6. Пользователям запрещается отправка в незащищенном виде электронных сообщений, содержащих государственную тайну, информацию о способах защиты сообщений можно получить в отделе по общим вопросам у системного администратора.

7. Вся исходящая почта, отправляемая внешним абонентам, не являющимся работниками администрации, архивируется и контролируется на предмет наличия информации, составляющей государственную или иную охраняемую законом тайну.

Приложение № 6

УТВЕРЖДЕНО
постановлением администрации
Буйского муниципального района
Костромской области
от 3 апреля 2019 г. № 111

Правила
использования системы Клиент-Банк в администрации Буйского муниципального района Костромской области

1. Общие положения

Настоящие правила вводятся в целях обеспечения соблюдения политики в сфере информационной безопасности, а также с целью предотвращения ненадлежащего использования компьютерного оборудования.

Настоящие правила устанавливают общие принципы, условия и порядок электронного документооборота с обслуживающими администрацию Буйского муниципального района Костромской области (далее – администрация) банками, осуществляемого с помощью системы «Клиент-Банк» (далее - СКБ).

Настоящие правила определяют права и обязанности пользователей СКБ, должностных лиц отдела по общим вопросам, обеспечивающих мероприятия по обеспечению информационной безопасности.

2. Описание программно-аппаратного комплекса СКБ

СКБ является информационной системой, организованной Банком и обеспечивающей взаимодействие Банка и клиента – администрации – с использованием технических средств в целях обеспечения электронного документооборота.

На стороне администрации СКБ содержит следующие компоненты:

- Клиентское программное обеспечение СКБ обслуживающего Банка, включая средства криптозащиты информации (СКЗИ). Допускается установка СКБ разных обслуживающих банков в рамках единого рабочего места.
- Системное программное обеспечение – операционная система, средства ограничения несанкционированного удаленного и/или непосредственного доступа к рабочему месту.
- Выделенный персональный компьютер с аппаратно-программными средствами защиты от несанкционированного доступа, изолированный от ресурсов корпоративной компьютерной сети администрации, подключенный к централизованному узлу доступа в сеть Интернет – рабочее место.
- Защищенная сеть передачи данных.
- Узел централизованного доступа в сеть Интернет.

Информационный обмен в рамках СКБ осуществляется по открытым каналам связи с использованием электронного документооборота по сети Интернет.

Электронный документооборот включает в себя процесс формирования электронного документа (далее - ЭД), подписание его электронно-цифровой

подписью (далее - ЭЦП) и/или цифровой подписью (далее - ЦП), передачу ЭД получателю, проверку ЭД на подлинность (проверка ЭЦП), а также учет и хранение ЭД.

В целях обеспечения электронного документооборота Банк осуществляет управление сертификатами ключей ЭЦП.

- Носители с ключами должны храниться в специально отведенном месте (сейфе) и устанавливаются в компьютер только на время работы с программой.
- Рабочее место СКБ должно быть снабжено парольным входом в компьютер. При необходимости перерыва в работе оператор должен выйти из программы и осуществить блокировку клавиатуры и экрана ПК средствами установленной системы защиты от несанкционированного доступа. После завершения работы выключить ПК, носители с ключами убрать в место хранения.
- В случае отсутствия владельца ЭЦП (отпуск, болезнь и т.д.) к обработке электронных документов с ЭЦП допускается ответственное лицо, назначенное распоряжением администрации.
- Плановая смена рабочих ключей происходит по согласованию с Банком.
- Ключевые носители с секретными ключами ЭЦП и шифрования (секретными ключами ЦП и кодирования), а также инсталляционные носители с программным обеспечением СКЗИ необходимо взять на поэкземплярный учет в выделенных для этих целей журналах;
- Рабочие комплекты ключей (и их копии) и комплекты резервных ключей хранятся раздельно с обеспечением условия невозможности их одновременной компрометации или уничтожения;
- Лица ответственные за учет и хранение секретных ключей назначаются распоряжением по администрации.

3. Порядок использования СКБ

3.1. Взаимодействие корпоративной информационной системы и СКБ

Подготовка платежного документа выполняется средствами корпоративной информационной системы администрации.

Сформированный документ сохраняется в виде выходного файла и записывается на сменный flash-носитель информации.

Сменный flash-носитель устанавливается в USB-порт рабочего места СКБ, содержащиеся на нем сформированные документы загружаются пользователем в клиентское программное обеспечение СКБ для последующего формирования электронных платежных документов.

Полученные из банка электронные документы аналогичным способом переносятся пользователем в корпоративную информационную систему, где ведется архив отправленных и полученных документов.

3.2. Использование СКБ

Использование программного обеспечения СКБ Банка необходимо осуществлять в соответствии с «Регламентом электронного документооборота», предоставляемым Банком.

3.3. Ситуации компрометации ключевой информации

Понятие компрометации означает, что произошло нарушение безопасности хранения и использования ключа, в результате которого возникла

вероятность несанкционированного его применения и нанесения тем самым ущерба администрации. К событиям, связанным с компрометацией ключей относятся:

- Утрата носителя (оригинал и/или дубликат) с закрытыми ключами;
- Утрата носителя (оригинал и/или дубликат) с закрытыми ключами с ее последующим обнаружением;
- Утрата ключей от сейфа в момент нахождения в нем носителей ключевой информации;
- Увольнение сотрудников, имевших доступ к ключевой информации;
- Носитель с закрытыми ключами стал на время доступен постороннему лицу без контроля со стороны владельца/пользователя;
- Обнаружен случай подписания электронного документа ЭЦП кем-либо, кроме самого владельца/пользователя ЭЦП;
- Нарушение печати на сейфе (контейнере, пенале) с ключами;
- Иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа к секретному ключу ЭЦП (ЦП) посторонних лиц.

При установлении факта компрометации действующих ключей должны быть приняты следующие меры:

- Поставить в известность управляющего делами администрации и (или) системного администратора отдела по общим вопросам администрации;
- Направить по каналу электронной связи в Банк текстовый файл с уведомлением (согласно Регламенту обслуживающего Банка) о компрометации ключей, которое подписывается скомпрометированной ЭЦП. При наличии резервных ключей, в уведомление необходимо добавить оповещение о переходе на использование резервных ключей;
- Немедленно прекратить обмен информацией с использованием скомпрометированных ключей. Формируется запрос на получение нового комплекта рабочих ключей;
- До получения новых рабочих ключей, для обмена данными с Банком применять резервные ключи, либо перейти на бумажный документооборот.

Выход из строя носителя с закрытыми ключами не рассматривается как компрометация ключей.

4. Права и обязанности пользователей СКБ

4.1. Пользователи СКБ

Пользователями СКБ являются сотрудники Администрации, выполняющие действия по проведению электронных платежей с ЭЦП в СКБ.

Список пользователей СКБ и возложение на них обязанности исполнения требований настоящих Правил в целях обеспечения информационной безопасности утверждается распоряжением администрации.

4.2. Пользователи обязаны:

- Осуществлять платежи с использованием СКБ в соответствии с утвержденным действующим финансовым планом (включая изменения и приложения к плану), а также при наличии первичных акцептованных документов в порядке очередности, указанной непосредственным руководителем.

Использовать клиентское программное обеспечение СКБ в соответствии с

«Регламентом электронного документооборота», предоставляемым Банком.

- В целях проведения электронных платежей с ЭЦП получить у представителя Банка два носителя (оригинал и копия) ключей для электронно-цифровой подписи, а также резервные ключи.
- В технологическом процессе использовать копию ключей, а в случае выхода ее из строя (механическое повреждение и т.д.) – оригинал, до создания новой копии ключа.
- Хранить ключи в опечатанном владельцем ЭЦП сейфе (контейнере, пенале). При хранении рабочих ключей в одном сейфе (металлическом шкафу) с другими документами они помещаются в отдельный опечатываемый контейнер. Условия хранения носителей с ключами должны исключать возможность коробления, изгиба под воздействием температуры или другим причинам, а также воздействия пыли, магнитных и электрических полей.
- Обеспечить сохранность ключей ЭЦП и шифрования (ЦП и кодирования), паролей для входа в СКБ и другой конфиденциальной информации от несанкционированного доступа.
- В целях обеспечения информационной безопасности пользователь обязуется соблюдать «Рекомендации клиенту СКБ по обеспечению безопасности информации при эксплуатации» - Приложение к договору об использовании СКБ Банка.
- Своевременно доводить до сведения системного администратора отдела по общим вопросам информацию об изменениях правил или режима работы СКБ, инициированных Банком, а также сроки и порядок вступления в силу этих изменений (не позднее, чем за десять рабочих дней до даты вступления в силу данных изменений и дополнений).

4.3. Пользователям запрещается:

- Выводить на монитор, печатающее устройство ключевую информацию (ключи);
- Не санкционированно изготавливать копии ключей;
- Передавать кому-либо носитель с ключами, flash-носитель с данными;
- Оставлять компьютер СКБ и носители с ключами без принятия мер по защите их от несанкционированного доступа.

4.4. Пользователи имеют право:

- Получать консультацию у специалистов отдела по общим вопросам, по работе с компьютерным оборудованием и программным обеспечением, по вопросам компьютерной безопасности;
- Вносить предложения по изменению настоящих правил;
- Получать уведомления об изменениях настоящих правил и правил работы на конкретном оборудовании.

5. Права и обязанности специалистов отдела по общим вопросам

5.1. Специалисты отдела по общим вопросам обеспечивают исправность оборудования и системного программного обеспечения СКБ, обеспечивают выполнение всех необходимых технических мероприятий для функционирования программного обеспечения клиентской части СКБ.

Ответственность за исправное функционирование оборудования и системного программного обеспечения СКБ, за соблюдение технических требований информационной безопасности в целях настоящих Правил

возлагается на системного администратора отдела по общим вопросам.

5.2. Системный администратор отдела по общим вопросам обязаны:

- Проверять исправность оборудования рабочего места СКБ, правильность функционирования программного обеспечения и соблюдение правил работы, с использованием, при необходимости, административного доступа на время проверки;
- По согласованию с главным бухгалтером администрации оперативно отключать компьютер СКБ от защищенной сети передачи данных, блокировать работу или выводить из эксплуатации оборудование в случае нарушения информационной безопасности, по причине неисправности оборудования или грубого нарушения Правил пользователями СКБ;
- Предоставлять пользователям СКБ информацию необходимую для работы на компьютерном оборудовании;
- Доводить до сведения пользователей СКБ информацию об изменении правил или режима работы СКБ, инициированных им по техническим причинам;
- Снижать до минимально необходимого время простоя оборудования вследствие неполадок или сервисных работ;
- Создавать копии рабочих ключевых носителей с секретными ключами ЭЦП и шифрования, которые будут использоваться в работе с СКБ в присутствии лица, ответственного за данную ЭЦП;
- Не разглашать информацию, полученную в ходе выполнения служебных обязанностей;

5.3. Системный администратор имеет право по согласованию с управляющим делами администрации имеет право:

- Проводить проверки содержимого компьютера СКБ на предмет его профильного использования;
- Делать предупреждения пользователям СКБ, нарушившим настоящие Правила;
- Доводить до сведения руководства пользователей СКБ факты грубого или неоднократно нарушения настоящих Правил;
- Требовать от пользователя СКБ подробного отчета о работе, если во время этой работы произошел отказ или сбой оборудования или программного обеспечения;
- Без предупреждения удалять с дисков СКБ файлы пользователей, содержащие игровые программы и программы, предназначенные для нарушения компьютерной безопасности, файлы, зараженные компьютерными вирусами, файлы, содержащие мультимедиа информацию, не имеющую отношения к профилю деятельности администрации с доведением до сведения своего непосредственного руководителя.

_____