МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
«ПАРК КУЛЬТУРЫ И ОТДЫХА «ВОЛЖСКИЙ»
ГОРОДСКОГО ОКРУГА – ГОРОД ВОЛЖСКИЙ
ВОЛГОГРАДСКОЙ ОБЛАСТИ

ПРИКАЗ

«04» мая 2022 г. № 43

Об утверждении внутренних нормативных актов
МАУ «ПКИО «Волжский» по защите информации

Во исполнение федеральных законов от 06.04.2011 № 63-ФЗ «Об электронной подписи», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в целях обеспечения информационной безопасности в муниципальном автономном учреждении «Парк культуры и отдыха «Волжский» городского округа - город Волжский Волгоградской области при работе

ПРИКАЗЫВАЮ:

1. Утвердить Положение об использовании средств криптографической защиты информации и электронной подписи (приложение 1).
2. Утвердить Положение о политике информационной безопасности (приложение 2).
3. Утвердить Положение о порядке организации и проведения работ по защите конфиденциальной информации (приложение 3).
4. Утвердить Инструкцию по антивирусной защите в информационных системах (приложение 4).
5. Утвердить Инструкцию по организации парольной защиты в информационной системе (приложение 5)
6. Утвердить Порядок учета, хранения и использования машинных носителей информации (приложение 6).
7. Утвердить Порядок разграничения доступа пользователей к обрабатываемой информации (приложение 7).
8. Утвердить Положение о подключении и использовании ресурсов информационно-телекоммуникационной сети Интернет (приложение 8).
9. Контроль за исполнением настоящего приказа оставляю за собой.

Директор А.Г. Минаев

Приложение 1
к приказу МАУ «ПКиО
«Волжский» от
04.05.22 № 23

Положение
об использовании средств криптографической защиты информации и электронной подписи в муниципальном автономном учреждении «Парк культуры и отдыха «Волжский» городского округа - город Волжский Волгоградской области

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с действующим законодательством Российской Федерации с целью совершенствования и упорядочения работы с электронными подписями (далее - ЭП) и повышения уровня защиты информации, используемой при работе МАУ «ПКиО «Волжский».

1.2. Настоящее Положение определяет:

- основные правила обращения с информационными системами и ключами электронной подписи, строгое выполнение которых необходимо для обеспечения защиты информации;

- порядок обеспечения правовых условий, при соблюдении которых в информационной системе электронная подпись признается юридически равносильной собственноручной (живой) подписи должностного лица, наделенного правом пользования электронной подписью.

1.3. Для авторизации и обеспечения достоверности документов и для обеспечения при необходимости конфиденциальности информации при передаче по открытым каналам связи используются средства криптографической защиты информации, сертифицированные в порядке, установленном законодательством Российской Федерации.

1.4. Под средством криптографической защиты информации (далее - СКЗИ) понимается средство вычислительной техники, которое осуществляет криптографическое преобразование информации для обеспечения ее безопасности.

1.5. Криптографические методы защиты позволяют обеспечить защиту целостности и авторства электронной информации с применением ЭП. Невозможность ввода информации от чужого имени (невозможность подделки ЭП) гарантируется при сохранении в тайне закрытого ключа ЭП пользователей.

1.6. Непрерывная организационная поддержка функционирования автоматизированного рабочего места (далее - АРМ) с ЭП предполагает обеспечение строгого соблюдения всеми пользователями требований информационной безопасности.

2. Порядок получения ЭП

2.1. Владельцы сертификата ключа проверки электронной подписи (далее - владельцы ЭП) назначаются приказом руководителя учреждения.

2.2. Владелец ЭП самостоятельно формирует закрытый ключ ЭП, а также запрос на получение сертификата открытого ключа (в электронном виде и на бумажном носителе).

2.3. Сертификаты ЭП выдаются владельцу ЭП в удостоверяющем центре. Владелец ЭП обязан самостоятельно обратиться к сотруднику, ответственному за ведение журнала поэкземплярного учета ЭП (приложение № 1), за фиксацией факта передачи ЭП.

3. Порядок хранения ЭП

3.1. Право доступа к рабочим местам с установленным программным обеспечением средств ЭП предоставляется только владельцам ЭП, специалисту по информационной

безопасности учреждения.

3.2. Использовать АРМ с установленными средствами ЭП необходимо в однопользовательском режиме. В отдельных случаях при необходимости использования АРМ несколькими лицами эти лица должны обладать равными правами доступа к информации.

3.3. Рекомендуется хранить ключевые носители в помещениях, которые имеют прочные входные двери с установленными на них надежными замками.

3.4. Для хранения электронных ключей и средств ЭП и шифрования в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами.

3.5. Хранение ключевых носителей допускается в одном хранилище с другими документами и ключевыми носителями, при этом отдельно от них и в упаковке, исключающей возможность негласного доступа к ним.

3.6. Транспортирование ключевых носителей за пределы организации допускается только в случаях, связанных с производственной необходимостью. Транспортирование ключевых носителей должно осуществляться способом, исключающим их утрату, подмену или порчу.

3.7. На технических средствах, оснащенных средствами ЭП, должно использоваться только лицензионное программное обеспечение фирм-производителей.

3.8. Должны быть приняты меры по исключению несанкционированного доступа к средствам ЭП, а именно:

- при загрузке операционной системы и при возвращении после временного отсутствия пользователя на рабочем месте должен запрашиваться пароль;
- ключевые носители, содержащие средства ЭП, не должны оставаться на рабочих местах без присмотра владельца ЭП;
- ключевой носитель извлекается из сейфа только на время работы с ЭП;
- при необходимости временно покинуть помещение, в котором проводятся работы с использованием ЭП, ключевой носитель должен быть вновь помещен в сейф.

3.9. При физической порче рабочего ключевого носителя пользователь подготавливает заявку на аннулирование сертификата ЭП и обращается к сотруднику, ответственному за ведение журнала поэкземплярного учета ЭП, для фиксации факта уничтожения ЭП.

4. Порядок использования ЭП, права и обязанности владельца ЭП

4.1. Владелец ЭП обязан:

- сохранять в тайне конфиденциальную информацию, ставшую ему известной в процессе работы со средствами ЭП, содержания средств ЭП, PIN-кодов для доступа к электронным ключам и средствам ЭП;
- обеспечить сохранность носителей ключевой информации и других документов, выдаваемых с ключевыми носителями;
- при работе с ключевыми документами руководствоваться действующим законодательством Российской Федерации, соответствующим регламентом удостоверяющего центра и настоящим Положением;
- обеспечивать надежное хранение секретных (закрытых) ключей шифрования и ЭП, исключать доступ к ним посторонних лиц;
- своевременно подавать заявления о приостановлении действия или аннулировании сертификата ключа проверки электронной подписи при порче ключевого носителя или наличии оснований полагать, что тайна ключа ЭП нарушена;
- обновлять сертификат ключа проверки ЭП при истечении его срока действия;
- своевременно фиксировать факты получения/уничтожения ЭП в журнале поэкземплярного учета ЭП.

4.2. Владелец ЭП также несет ответственность за то, чтобы на АРМ, на котором установлены средства ЭП, не были установлены и не эксплуатировались программы, которые могут нарушить функционирование программных средств и средств ЭП.
При обнаружении на рабочем месте, оборудованном средствами ЭП, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена, а владелец ЭП обязан немедленно сообщить об этом ответственному за учет средств криптографической защиты информации и электронных подписей для последующего устранения нарушений.

1.1. Владельцу ЭП запрещается:

- разглашать содержимое электронных носителей или передавать сами носители лицам, к ним не допущенным;
- вносить какие-либо изменения в программное обеспечение и средства ЭП;
- осуществлять несанкционированное копирование ключевых носителей;
- записывать на ключевые носители постороннюю информацию;
- использовать ключевые носители в режимах, не предусмотренных правилами пользования ЭП, либо использовать ключевые носители на посторонних компьютерах.

1.2. Владелец ЭП имеет право:

- обращаться к ответственному за учет средств криптографической защиты информации и электронных подписей за получением ключевых носителей, предназначенных для записи ЭП, установкой необходимого программного обеспечения для работы с ЭП;
- обращаться к ответственному за учет средств криптографической защиты информации и электронных подписей за консультацией по вопросам получения ЭП и разъяснения правил хранения и использования ЭП, получением лицензий СКЗИ для дальнейшей работы с ЭП.

2. Действия при компрометации ЭП

2.1. Под компрометацией ключа ЭП понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

2.2. К событиям, связанным с компрометацией ключей, относятся:

- потеря ключевых носителей;
- потеря ключевых носителей с последующим обнаружением;
- нарушение правил хранения и уничтожения (после окончания срока действия ключа);
- возникновение подозрений на утечку информации или ее искажение;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

2.3. При компрометации ключа владелец ЭП обязан незамедлительно обратиться в удостоверяющий центр, выпустивший ключ ЭП, с заявлением на аннулирование (отзыв) сертификата ключа ЭП.

3. Порядок уничтожения ЭП на ключевых носителях

3.1. Ключи должны быть выведены из действия и уничтожены в следующих случаях:

- плановая смена ключей;
- изменение реквизитов владельца ЭП;
- компрометация ключей;
- выход из строя (износ, порча) ключевых носителей;
- прекращение полномочий владельца ЭП.

3.2. Уничтожение ключей может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) ключей без повреждения ключевого носителя. Ключи стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (Touch Memory, Rutoken, eToken и т.п.).

3.3. Непосредственные действия по стиранию ключевой информации регламентируются эксплуатационной и технической документацией.

3.4. ЭП должна быть уничтожены не позднее 10 суток после вывода ее из действия (окончание срока действия, прекращение полномочий владельца ЭП, компрометация). Факт уничтожения оформляется путем составления акта и отражается в журнале учета поэкземплярного учета ЭП.

4. Порядок использования СКЗИ

4.1. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат учету в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых носителей.

4.2. Дистрибутив программного обеспечения рекомендуется хранить в помещениях, которые имеют прочные входные двери с установленными на них надежными замками.

4.3. Для хранения в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами.

5.Обязанности ответственного за учет средств криптографической защиты информации и электронных подписей

5.1. Ответственный за учет средств криптографической защиты информации и электронных подписей:

- получает СКЗИ для сотрудников учреждения;
- заносит данные о СКЗИ в журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых носителей (приложение № 2);
- заносит данные об ЭП в журнал поэкземплярного учета ЭП;
- консультирует пользователей о правилах получения ЭП;
- заполняет акт уничтожения ЭП (приложение №3) при обращении пользователя ЭП за фиксацией факта истечения срока пользования ЭП, компрометации ЭП и в иных случаях, при которых использование ЭП не допускается.
- устанавливает СКЗИ, ЭП на АРМ пользователей;
- заполняет акт установки СКЗИ (приложение № 4);
- контролирует целостность аппаратных средств и программных продуктов, в которых используется ЭП;
- выдает съемные носители пользователям для записи ЭП.

Директор А.Г. Минаев

Приложение № 2
к Положению об использовании средств криптографической защиты информации и электронной подписи в МАУ «ПКиО «Волжский»

Журнал

поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых носителей

Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
			От кого получены	Дата и номер сопроводительного письма	Ф.И.О. Пользователя СКЗИ	Дата и расписка получения	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших изъятие (уничтожение)	Номер акта или расписка об уничтожении	

Приложение № 1
к Положению об использовании средств криптографической защиты информации и электронной подписи в МАУ «ПКиО «Волжский»

Журнал поэкземплярного учета электронных подписей

Наименование ЭД ключевого документа	Серийный номер ЭД номера серии ключевых документов	Номера экземпляров ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении ЭЦП			Отметка об изъятии ЭЦД уничтожении ключевых документов			примечание
			От кого получены	Дата, № сопроводительного письма	ФИО пользователя ЭП	Дата, подпись о получении	Ф И О сотрудника, произведшего подключение ЭП	Дата, подпись лица, произведшего подключение ЭП	Номера аппаратных средств, в которые установлены ЭП	Дата изъятия	Ф И О сотрудника, произведшего изъятие ЭП	№ акта, письма об уничтожении	
2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение № 3
к Положению об использовании средств криптографической защиты информации и электронной подписи в МАУ «ПКиО «Волжский»

АКТ
на уничтожение электронной подписи

(наименование организации)

г. Волжский « » 20 г.

Настоящий акт составлен о том, что в присутствии владельца ЭП по причине _____
_____ уничтожены закрытые ключи ЭП:
(окончания срока действия, прекращения полномочий, компромстации)

№ п/п	Ключевой носитель	Серийный номер электронной подписи	Ф.И.О. владельца ЭП

Владелец электронной подписи _____ (подпись) _____ (Ф.И.О.)

Ответственный за учет средств криптографической защиты информации и электронных подписей _____ (подпись) _____ (Ф.И.О.)

Директор _____ (подпись) _____ (Ф.И.О.)

(

Приложение № 4
к Положению об использовании средств криптографической защиты информации и электронной подписи в МАУ «ПКиО «Волжский»

АКТ №_____
установки средств криптографической защиты информации
в МАУ «ПКиО «Волжский»

г. Волжский «__»_____ 20 г.

Настоящий акт составлен о том, что _____ в присутствии
(дата)
пользователя СКЗИ _____
_____
(должность, фамилия, имя, отчество)
была произведена установка СКЗИ _____
_____
_____
_____
_____
(серийный номер СКЗИ, регистрационный номер ключевого носителя)
на автоматизированное рабочее место _____
_____
_____
_____
(структурное подразделение, кабинет, инвентарный номер аппаратных средств)
_____
_____
_____
_____
(фамилия, имя, отчество, должность сотрудника, произведшего установку)

Ответственный за учет средств
криптографической защиты информации и
электронных подписей _____ _____
(подпись) (Ф.И.О.)

Пользователь СКЗИ _____ _____
(подпись) (Ф.И.О.)

Приложение 2
к приказу
МАУ «ПКиО «Волжский» от
04 05 22 № 23

Положение
о политике информационной безопасности в муниципальном автономном учреждении
«Парк культуры и отдыха «Волжский» городского округа – город Волжский
Волгоградской области

1. Общие положения

1.1. Положение о политике информационной безопасности муниципального автономного учреждения «Парк культуры и отдыха «Волжский» городского округа – город Волжский Волгоградской области (далее Положение) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области информационной безопасности, которыми руководствуется муниципальное автономное учреждение «Парк культуры и отдыха «Волжский» городского округа – город Волжский Волгоградской области (далее МАУ «ПКиО «Волжский») в своей деятельности.

1.2. Основными целями политики информационной безопасности МАУ «ПКиО «Волжский» (далее политика) являются защита информации и обеспечение эффективной работы всей информационно-вычислительной системы МАУ ПКиО «Волжский».

1.3. Ведение деятельности по информационной безопасности (разработка нормативно-правовых актов и иной документации в области защиты информации, ведение журналов, техническая защита информации, разработка методов защиты информации и т. п.) в МАУ «ПКиО «Волжский» осуществляет уполномоченный сотрудник учреждения.

1.4. Контроль за соблюдением требований по информационной безопасности в МАУ «ПКиО «Волжский» обеспечивает руководитель учреждения.

1.5. Расследование инцидентов информационной безопасности осуществляет комиссия по расследованию и реагированию на инцидент информационной безопасности. которая создается и собирается в учреждении.

1.6. Сотрудники МАУ «ПКиО «Волжский» обязаны соблюдать порядок обращения с документами, содержащими защищаемую информацию, ключевыми носителями. следовать требованиям настоящего Положения и иных документов. регламентирующих деятельность в области информационной безопасности

2. Основные термины и сокращения

2.1. В настоящем Положении используются следующие термины и определения:

- автоматизированная система (далее АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;
- информационная система (далее ИС) - совокупность содержащейся в базах данных информации;
- ответственный за информационную безопасность (далее ОИБ) - лицо или группа лиц, ответственных за обеспечение организационно-правовых мер информационной безопасности АС и ИС, за реализацию технической защиты АС и ИС, бесперебойной и непрерывной работы серверного оборудования, на котором обрабатываются АС и ИС, восстановление баз данных АС и ИС до работоспособного состояния при успешных попытках несанкционированного доступа (далее НСД);

- вредоносная программа - программа, предназначенная для осуществления НСД и (или) воздействия на информацию конфиденциального характера или ресурсы АС и ИС;
- НСД - доступ к информации или действия с информацией, нарушающие правила разграничения доступа;
- средства вычислительной техники - совокупность программных и технических элементов систем обработки информации, способных функционировать самостоятельно или в составе других систем;
- доступ к информации - возможность получения информации и ее использования;
- защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;
- информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- целостность информации- способность средства вычислительной техники или АС обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения);
- пользователь ИС - лицо, участвующее в функционировании ИС или использующее результаты ее функционирования;
- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

3. Цели и задачи политики

3.1. Основными целями информационной безопасности МАУ «ПКиО «Волжский» являются:
- повышение стабильности функционирования АС и ИС МАУ «ПКиО «Волжский»;
- достижение адекватности мер по защите от реальных угроз информационной безопасности;
- предотвращение или снижение ущерба от инцидентов нарушения информационной безопасности.

3.2. Основными задачами деятельности по обеспечению информационной безопасности МАУ «ПКиО «Волжский» являются:
- выполнение требований действующего законодательства Российской Федерации по обеспечению информационной безопасности;
- контроль за выполнением установленных требований по обеспечению информационной безопасности;
- разработка и совершенствование организационно-распорядительных документов МАУ «ПКиО «Волжский» в области обеспечения информационной безопасности;
- выявление, оценка и прогнозирование угроз информационной безопасности;
- выработка рекомендаций по устранению уязвимых мест системы информационной безопасности;
- организация технической защиты АС и ИС от НСД и утечки по техническим каналам связи.

4. Объекты защиты

4.1. Основными объектами системы информационной безопасности в МАУ

«ПКиО «Волжский» являются:

- управленческий процесс;
- межведомственное взаимодействие;
- финансово-экономическая информация;
- информационный технологический процесс;
- информация ограниченного распространения, не составляющая государственную тайну.

4.2. Информация ограниченного распространения, не составляющая государственную тайну, обрабатываемая в ИС МАУ «ПКиО «Волжский», состоит из:

- сведений, содержащихся в личных делах сотрудников;
- сведений, раскрывающих систему, средства и методы защиты информации на средствах вычислительной техники от НСД, а также значений действующих логинов и паролей;
- сведений, содержащихся в материалах по аттестации технических средств и систем, предназначенных для защиты или обработки конфиденциальной информации;
- других служебных сведений, доступ к которым ограничен в соответствии с действующим законодательством Российской Федерации.

5. Основные принципы обеспечения информационной безопасности

5.1. Основными принципами обеспечения информационной безопасности являются:

- постоянный и всесторонний анализ АС и информационных технологий с целью выявления уязвимостей информационных активов МАУ «ПКиО «Волжский»;
- своевременное обнаружение проблем, потенциально способных повлиять на информационную безопасность МАУ «ПКиО «Волжский», корректировка моделей угроз;
- разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию и совместимости этих мер с действующим технологическим процессом;
- контроль эффективности принимаемых защитных мер.

6. Модель угроз и модель нарушителей

6.1. Модель угроз используется для анализа защищенности ИС МАУ «ПКиО «Волжский» и разработки системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз.

6.2. По признаку принадлежности к ИС все нарушители делятся на две группы:

- внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается ИС;
- внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается ИС.

6.2.1. Внешним нарушителем может быть лицо из следующих категорий:

- уволенные сотрудники;
- представители организаций, взаимодействующих по вопросам технического обеспечения;
- посетители;
- другие лица, заинтересованные в нарушении целостности, доступности и конфиденциальности информации.

6.2.2. Внутренним нарушителем может быть лицо из следующих категорий сотрудников МАУ «ПКиО «Волжский»:

- пользователи ИС;
- сотрудники, не являющиеся пользователями ИС, но имеющие доступ в здания и помещения;

- технический персонал (уборщики, охранники и т. п.).

7. Методы и средства обеспечения информационной безопасности

7.1. Обеспечение информационной безопасности МАУ «ПКиО «Волжский» реализуется принятием следующих мер защиты:

- организационно-правовых;
- технических;
- физических.

7.2. Меры защиты призваны обеспечить:

- конфиденциальность информации (защита от несанкционированного ознакомления);
- целостность информации (защищенность от разрушения и несанкционированного изменения);
- доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

7.3. Организационно-правовой мерой защиты информации является создание и утверждение организационно-распорядительной документации (далее ОРД).

К такой ОРД относятся:

- общие документы, регламентированные для исполнения Федеральных законов, постановлений правительства, приказов Федеральной службы безопасности и Федеральной службы по техническому и экспортному контролю Российской Федерации и иных подзаконных актов.
- документы, которые необходимы для функционирования ИС;
- документы по защите персональных данных;
- документы, необходимые для использования средств криптографической защиты информации (далее СКЗИ).

7.4. Технической мерой защиты информации является обеспечение целостности охраняемой информации от НСД со стороны информационно-телекоммуникационной сети Интернет и локально-вычислительной сети учреждения с использованием средств защиты информации (далее СЗИ). К таким СЗИ относятся:

- СКЗИ;
- межсетевой экран (далее МСЭ);
- файрволы и брандмауэры;
- антивирусное программное обеспечение;
- средства разграничения доступа;
- средства регистрации событий безопасности;
- средства восстановления целостности баз данных и операционной среды.

7.4.1. В целях предотвращения работы посторонних лиц с информационными ресурсами МАУ «ПКиО «Волжский» необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей).

7.4.1.1. Аутентификация (подтверждение подлинности) пользователей может осуществляться:

- путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей и т.д.);
- путем проверки знания ими логинов и паролей.

7.4.2. Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа к:

- компонентам информационной среды и элементам системы защиты информации (физический доступ);
- информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);
- активным ресурсам (прикладным программам, задачам и т.п.);

- операционной системе, системным программам и программам защиты.

7.4.3. Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, МСЭ, файрволы и брандмауэры, программы восстановления целостности операционной среды и баз данных.

7.4.3.1. Средства контроля целостности информационных ресурсов системы предназначены для предупреждения и своевременного обнаружения вредоносного кода, модификаций или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

7.4.4. Средства регистрации событий безопасности должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей и т. п.), которые могут привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации.

7.4.4.1. Средства контроля и регистрации должны предоставлять возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов);
- получения твердой копии (печати) журнала регистрации событий безопасности;
- упорядочения журналов, а также установления ограничений на срок их хранения;
- оперативного оповещения ОИБ о нарушениях.

7.4.5. Элементами системы обеспечения безопасности информации МАУ «ПКиО «Волжский» являются СКЗИ.

7.4.5.1. Конфиденциальность и защита информации при ее передаче по каналам связи должна обеспечиваться также за счет применения в системе шифросредств абонентского шифрования.

7.5 Физические меры защиты информации основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

7.5.1. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в них посторонних лиц, хищение документов и носителей информации, самих средств информатизации, а также исключающими нахождение внутри контролируемой зоны технических средств съема информации.

7.5.2. Для обеспечения физических мер безопасности защищаемой информации МАУ «ПКиО «Волжский» необходимо осуществлять ряд мероприятий, включающих проверку оборудования, предназначенного для обработки защищаемой информации, на:

- наличие специально внедренных закладных устройств;
- побочные электромагнитные излучения и наводки;
- введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки информации ограниченного доступа, не составляющей государственную тайну;
- оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

8. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов информационной безопасности

8.1. К техническим мерам обеспечения непрерывной работы и восстановления ресурсов относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

8.2. Системы жизнеобеспечения включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

8.2.1. Все критичные помещения МАУ «ПКиО «Волжский» (помещения, в которых размещаются элементы АС и ИС и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

8.2.2. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы АС, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания.

8.3. Для обеспечения отказоустойчивости критичных компонентов АС и ИС при сбое в работе оборудования и их автоматической замены без простоев должна использоваться технология резервного копирования. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, применяется дублирование данных, хранимых на дисках.

8.3.1. Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для информации, содержащей сведения ограниченного распространения, - не реже одного раза в месяц;
- для технологической информации - не реже одного раза в три месяца;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС - не реже одного раза в полгода и каждый раз при внесении изменений в эталонные копии (выход новых версий).

9. Управление информационной безопасностью

9.1. Управление информационной безопасностью МАУ «ПКиО «Волжский» включает в себя:

- разработку регламентирующих и методических документов обеспечения информационной безопасности;
- обеспечение штатного функционирования комплекса средств информационной безопасности;
- осуществление контроля за функционированием системы информационной безопасности;
- обучение с целью поддержки (повышения) квалификации персонала МАУ «ПКиО «Волжский»;
- оценку рисков, связанных с нарушением информационной безопасности.

9.2. Основными направлениями по обеспечению информационной безопасности являются:

- разработка технических, организационных и административных планов реализации политики информационной безопасности;
- проведение единой технической политики, организация и координация работ по защите информации;
- подготовка рекомендаций по выбору средств защиты информации;

- администрирование средств защиты информации в части обеспечения работоспособности прикладного программного обеспечения и их обновления;
- участие в обеспечении бесперебойной работы АС и восстановлении работы после сбоев;
- обучение пользователей безопасной работе с информационными активами;
- контроль за соблюдением требований по использованию антивирусных средств;
- организация аттестации объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности и/или конфиденциальности;
- организация и проведение работ по контролю эффективности проводимых мероприятий и принимаемых мер по защите информации;
- разработка предложений по организации и совершенствованию системы защиты информации;
- подготовка отчетов о состоянии работы по защите информации.

9.3. Ответственные структурных подразделений МАУ «ПКиО «Волжский» обеспечивают соблюдение положений и документов по защите информации.

10. Контроль за соблюдением настоящего Положения

10.1. Контроль состояния информационной безопасности осуществляется сотрудниками МАУ «ПКиО «Волжский», ответственными за обеспечение мер по защите информации.

10.2. Контроль эффективности средств по защите необходимо осуществлять не реже одного раза в год. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы средств защиты (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т. п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности ИС.

10.3. Мероприятия по осуществлению контроля включают в себя:
- контроль за соблюдением режима защиты;
- контроль за соблюдением режима обработки информации, содержащей сведения ограниченного распространения;
- контроль за выполнением антивирусной защиты;
- контроль за соблюдением режима защиты при подключении к сетям общего пользования;
- контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИС;
- контроль за обеспечением резервного копирования;
- организация анализа и пересмотра имеющихся угроз безопасности ИС, а также предсказание появления новых, еще неизвестных, угроз;
- поддержание в актуальном состоянии нормативно-организационных документов.

Директор А.Г. Минаев

Приложение 3
к приказу МАУ «ПКиО «Волжский»
от 04.05.22 № 23

Положение
о порядке организации и проведения работ по защите конфиденциальной информации

1. Общие положения

1.1. Настоящее Положение определяет порядок организации и проведения работ по защите конфиденциальной информации в муниципальном автономном учреждении «Парк культуры и отдыха «Волжский» городского округа - город Волжский Волгоградской области (далее МАУ «ПКиО «Волжский»).

1.2. Мероприятия по защите конфиденциальной информации, проводимые в МАУ «ПКиО «Волжский», являются составной частью управленческой и иной служебной деятельности и осуществляются во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ.

1.3. Информационные системы и ресурсы МАУ «ПКиО «Волжский» подлежат обязательному учету и защите.

1.4. Конфиденциальная информация должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической защиты конфиденциальной информации.

1.5. Уровень технической защиты конфиденциальной информации, а также перечень необходимых мер защиты определяется дифференцировано по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты конфиденциальной информации и величины ущерба, который может быть нанесен собственнику конфиденциальной информации при ее разглашении, утрате, уничтожении и искажении.

1.6. Системы и средства информатизации и связи, предназначенные для обработки (передачи) конфиденциальной информации, должны быть аттестованы в реальных условиях эксплуатации на предмет соответствия принимаемых мер и средств защиты требуемому уровню безопасности информации.

1.7. Проведение любых мероприятий и работ с конфиденциальной информацией без принятия необходимых мер технической защиты информации не допускается.

1.8. Объектами защиты в МАУ «ПКиО «Волжский» являются:

- средства и системы информатизации и связи (средства вычислительной техники, локальная вычислительная сеть (ЛВС), средства и системы связи и передачи информации, переговорные устройства, средства изготовления и тиражирования документов, используемые для обработки, хранения и передачи информации, содержащей конфиденциальную информацию, - основные технические средства и системы (далее ОТСС);
- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается конфиденциальная информация, - вспомогательные технические средства и системы (далее ВТСС);
- помещения (служебные кабинеты, актовые, конференц-залы и т.п.), специально предназначенные для проведения конфиденциальных мероприятий, - защищаемые помещения (далее ЗП).

2. Технические каналы утечки конфиденциальной информации, несанкционированного доступа и специальных воздействий на нее

2.1. Доступ к конфиденциальной информации, нарушение ее целостности и доступности возможно реализовать за счет:

- несанкционированного доступа к конфиденциальной информации при ее обработке в информационных системах и ресурсах;
- утечки конфиденциальной информации по техническим каналам.

2.2. Детальное описание возможных технических каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на нее содержится в Модели угроз безопасности информации МАУ «ПКиО «Волжский».

3. Оценка возможностей технических разведок и других источников угроз безопасности конфиденциальной информации

3.1. Для добывания конфиденциальных сведений могут использоваться:
- портативная возимая (носимая) аппаратура радио-, акустической, визуальнооптической и телевизионной разведки, а также разведки побочных электромагнитных излучений и наводок (далее ПЭМИН);
- автономная автоматическая аппаратура акустической и телевизионной разведки, а также разведки ПЭМИН;
- компьютерная разведка, использующая различные способы и средства несанкционированного доступа к информации и специальных воздействий на нее.

3.2. Угроза компьютерной разведки объектам защиты возможна в случае подключения автоматизированных систем (далее АС), обрабатывающих информацию ограниченного доступа, к внешним, в первую очередь, глобальным сетям.

3.3. Портативная возимая аппаратура разведки может применяться из ближайших зданий и автомобилей на стоянках вблизи зданий.

3.4. Портативная носимая аппаратура имеет ограниченные возможности и может быть использована лишь для уточнения данных или перехвата информации в непосредственной близости от защищаемых объектов.

3.5. Автономная автоматическая аппаратура радио-, акустической, телевизионной разведки, а также разведки ПЭМИН используется для длительного наблюдения за объектом защиты.

3.6. Несанкционированный доступ (далее НСД) к информации и специальные воздействия на нее могут осуществляться при ее обработке на отдельных автоматизированных рабочих местах, в локальных вычислительных сетях, в распределенных телекоммуникационных системах.

3.7. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны (далее КЗ). Это возможно, например, вследствие:
- непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций, защищаемых помещений и их инженерно-технических систем;
- случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;
- некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;
- просмотра информации с экранов дисплеев и других средств ее отображения.

3.8. Оценка возможностей средств технической разведки осуществляется с использованием нормативных документов ФСТЭК России.

3.9. Наиболее опасной является аппаратура портативной (возимой и носимой) разведки электромагнитных излучений и аппаратура акустической речевой разведки, которая может применяться с прилегающей к зданиям МАУ «ПКиО «Волжский» территории, а также автономная автоматическая аппаратура акустической речевой разведки, скрытно устанавливаемая внутри помещений.

3.10. Оценка возможности НСД к информации в средствах вычислительной техники и автоматизированных системах осуществляется с использованием руководящих документов ФСТЭК России.

3.11. НСД к информации и специальные воздействия на нее реально возможны. если не выполняются требования перечисленных выше документов, дифференцированные в зависимости от степени конфиденциальности обрабатываемой информации, уровня полномочий пользователей по доступу к конфиденциальной информации и режимов обработки данных в автоматизированных системах.

4. Организационные и технические мероприятия по технической защите конфиденциальной информации

4.1. Разработка организационно-правовых мер в МАУ «ПКиО «Волжский» осуществляется ответственным за обеспечение информационной безопасности учреждения

4.2. Для защиты конфиденциальной информации используются сертифицированные по требованиям безопасности технические средства защиты.

4.3. Объекты информатизации должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.

4.4. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на должностное лицо, эксплуатирующее объекты информатизации.

4.5. Порядок организации антивирусной защиты конфиденциальной информации при ее обработке техническими средствами в МАУ «ПКиО «Волжский» определен инструкцией по организации антивирусной защиты информации.

4.6. Порядок организации парольной защиты конфиденциальной информации при ее обработке техническими средствами в МАУ «ПКиО «Волжский» определен инструкцией по организации парольной защиты.

5. Обязанности и права должностных лиц

5.1. Ответственный за обеспечение информационной безопасности учреждения обеспечивает техническую защиту информации, циркулирующую в технических средствах и помещениях учреждения.

5.2. Владельцы и пользователи ОТСС обеспечивают уровень технической защиты информации в соответствии с требованиями (нормами), установленными в нормативных документах.

5.3. Владельцы и пользователи ОТСС обязаны вносить предложения о приостановке работ с использованием сведений, составляющих конфиденциальную или служебную тайну, в случае обнаружения утечки (или предпосылок к утечке) этих сведений.

6. Контроль состояния технической защиты конфиденциальной информации

6.1. Существуют два относительно самостоятельных направления защиты информации от НСД: направление, связанное с СВТ, и направление, связанное с АС.

6.2. Защита СВТ обеспечивается комплексом программно-технических средств Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

Директор А.Г. Минаев

Приложение 4
к приказу МАУ «ПКиО «Волжский»
от 04 05 22 № 23

ИНСТРУКЦИЯ

по антивирусной защите в информационных системах в муниципальном автономном учреждении «Парк культуры и отдыха «Волжский» городского округа - город Волжский Волгоградской области

1. Общие положения

1.1 Настоящая Инструкция предназначена для всех сотрудников в муниципальном автономном учреждении «Парк культуры и отдыха «Волжский» городского округа - город Волжский Волгоградской области (далее - МАУ «ПКиО «Волжский»), имеющих доступ к информационным системам (ИС) МАУ «ПКиО «Волжский».

1.2 Инструкция устанавливает требования и ответственность при организации защиты информации от воздействия вредоносных компьютерных вирусов.

1.3 Инструкция регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля при работе в ИС МАУ «ПКиО «Волжский».

2. Обеспечение антивирусной защиты

2.1 Порядок организации антивирусной защиты.

2.1.1 Для организации антивирусной защиты ИС МАУ «ПКиО «Волжский» допускаются к использованию только сертифицированные ФСТЭК России лицензионные антивирусные средства общего применения.

2.1.2 Антивирусное средство защиты должно быть установлено на все средства вычислительной техники (СВТ) (при наличии технической возможности), входящие в ИС МАУ «ПКиО «Волжский».

2.1.3 В ИС МАУ «ПКиО «Волжский» права по управлению (администрированию) средствами антивирусной защиты предоставлены только ответственному за обеспечение информационной безопасности учреждения .

2.1.4 Разработка и осуществление мероприятий по проведению антивирусного контроля осуществляется ответственным за защиту информации с привлечением (при необходимости) специалистов лицензированной организации.

2.1.5 Должностные лица не должны допускать использования в ИС МАУ «ПКиО «Волжский» программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

2.1.6 В ИС МАУ «ПКиО «Волжский» обеспечивается централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (автоматизированных

договор на антивирусную поддержку (при наличии);

– по факту обнаружения зараженных вирусом файлов составить служебную записку директору, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

2.3 Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

2.3.1 Ответственный за обеспечение информационной безопасности учреждения обеспечивает получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

2.3.2 Контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов) обеспечивается путем автоматического получения или предварительно скачиваемых обновлений из официальных источников, например, с сервера обновлений производителя антивирусного средства.

3. Ответственность при организации антивирусной защиты

3.1 Ответственность за организацию антивирусной защиты ИС МАУ «ПКиО «Волжский» в соответствии с требованиями настоящей Инструкции возлагается на ответственного за обеспечение информационной безопасности учреждения.

3.2 Ответственность за соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение информационной безопасности учреждения ИС МАУ «ПКиО «Волжский», и пользователей, эксплуатирующих ИС МАУ «ПКиО «Волжский».

Директор А.Г. Минаев

Приложение 5
к приказу МАУ «ПКиО «Волжский» от
04 05 22 № 23

ИНСТРУКЦИЯ

по организации парольной защиты в информационной системе в муниципальном автономном учреждении «Парк культуры и отдыха «Волжский» городского округа - город Волжский Волгоградской области

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в муниципальном автономном учреждении «Парк культуры и отдыха «Волжский» городского округа - город Волжский Волгоградской области, а также контроль над действиями пользователя при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на ответственного за обеспечение информационной безопасности учреждения.

2. Личный пароль должен выбираться и генерироваться пользователем ИС самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее шести символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (ЭВМ, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владелец пароля должен быть ознакомлен под роспись с перечисленными выше требованиями и предупрежден об ответственности за использование пароля, не соответствующего данным требованиям, а также за разглашение парольной информации.

3. При возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передать руководителю подразделения. Опечатанные конверты с паролями исполнителей должны храниться в сейфе у руководителя.

4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 6 месяцев.

5. Внеплановая смена личного пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться ответственным за обеспечение информационной безопасности ИС немедленно после окончания последнего сеанса работы данного пользователя с системой.

6. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) ответственного за обеспечение информационной безопасности ИС.

7. В случае компрометации личного пароля пользователя ИС должны быть немедленно предприняты меры в соответствии с п.5 или п.6 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

8. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в сейфе руководителя.

9. Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственного за обеспечение информационной безопасности ИС.

Директор А.Г. Минаев

Приложение 6
к приказу МАУ «ПКиО «Волжский»
от 04.05.22 № 23

Порядок
учета, хранения и использования машинных носителей информации в муниципальном автономном учреждении «Парк культуры и отдыха «Волжский» городского округа - город Волжский Волгоградской области

1. Общие положения

1.1. Настоящий Порядок определяет порядок учета, хранения и использования машинных носителей информации в МАУ «ПКиО «Волжский».

1.2. В МАУ «ПКиО «Волжский» применяются машинные носители информации следующих типов:

- накопители на жестких магнитных дисках (далее НЖМД);
- электронные накопители информации (USB-флэш-накопители);
- оптические диски однократной и многократной записи.

2. Учет машинных носителей

2.1. Все типы и виды используемых и находящихся на хранении машинных носителей подлежат учету (приложение № 1).

2.2. Каждому машинному носителю присваивается учетный номер. В качестве учетных номеров могут использоваться серийные номера машинных носителей, присвоенные производителями машинных носителей информации, номера инвентарного учета.

2.3. Если на автоматизированном рабочем месте (далее АРМ) используются технические средства с несколькими встроенными машинными носителями, то каждому машинному носителю присваивается отдельный учетный номер.

2.4. Учет машинных носителей осуществляет юридическое лицо - правомерный владелец машинных носителей.

2.5. В случае если МАУ «ПКиО «Волжский» машинные носители предоставляет сторонняя организация, между ними должно быть заключено соглашение о взаимодействии.

3. Использование машинных носителей

3.1. Под использованием машинных носителей понимается их подключение к АРМ с целью обработки, приема и (или) передачи информации между информационными системами и машинным носителем.

3.2. Машинные носители предоставляются сотрудникам МАУ «ПКиО «Волжский» в случаях необходимости выполнения ими своих должностных обязанностей или возникновения производственной необходимости.

3.3. НЖМД разрешается подключать к АРМ только ответственному за обеспечение информационной безопасности учреждения.

3.4. Машинные накопители запрещается выносить за пределы МАУ «ПКиО «Волжский» без служебной необходимости.

3.5. При использовании машинных носителей необходимо:

- соблюдать требования настоящего Порядка;
- использовать машинные носители исключительно для выполнения своих должностных обязанностей;
- бережно относиться к машинным носителям, обеспечивать их физическую безопасность;

- информировать ответственного за обеспечение информационной безопасности учреждения либо иное лицо, ответственное за обеспечение информационной безопасности, о фактах утери, порчи машинных носителей и о любых фактах нарушения требований настоящего Порядка.

3.6. При использовании машинных носителей запрещается:

- использовать машинные носители в личных целях;
- передавать машинные носители на хранение или использование третьим лицам;
- использовать съемные носители информации, не внесенные в список разрешенных к использованию.

3.7. Машинные носители перед использованием подлежат обязательной проверке на отсутствие вредоносного программного обеспечения.

3.8. Любое взаимодействие, инициированное сотрудником между информационными системами МАУ «ПКиО «Волжский» и неучтенными (личными) машинными носителями, рассматривается как несанкционированное.

3.9. В случае выявления фактов несанкционированного и/или нецелевого использования машинных носителей ответственный за обеспечение информационной безопасности учреждения вправе инициировать служебную проверку.

3.10. Машинные носители, пришедшие в негодность или отслужившие установленный срок эксплуатации, подлежат снятию с учета, очистке и уничтожению.

3.11. По результатам уничтожения машинных носителей составляется акт и в журнал учета (приложение) вносятся соответствующие записи.

3.12. При передаче средств вычислительной техники, содержащих учтенные машинные носители, для проведения ремонтно-восстановительных или иных работ машинные носители изымаются из состава средства вычислительной техники.

3.13. В случае увольнения сотрудника предоставленные ему машинные носители изымаются и форматируются, в журнал учета вносится соответствующая запись.

4. Ответственность

Каждый сотрудник МАУ «ПКиО «Волжский» несет персональную ответственность за использование и сохранность машинных носителей, принятых им и зарегистрированных в журнале учета, за несоблюдение положений настоящего Порядка и неправомерное использование машинных носителей.

Директор А.Г. Минаев

Приложение1
к Порядку учета, хранения и использования машинных носителей информации в МАУ «ПКиО «Волжский»

Журнал учета, хранения и использования машинных носителей информации

Порядковый номер	Серийный номер машинного носителя	Место установки (использования)	Структурное подразделение	Ф.И.О. ответственного сотрудника	Отметка о получении ответственным сотрудником	Отметка об уничтожении	Примечание

Приложение7
к приказу МАУ «ПКиО «Волжский»
от 04 05 22 № 43

Порядок

разграничения доступа пользователей к обрабатываемой информации в муниципальном автономном учреждении «Парк культуры и отдыха «Волжский» городского округа - город Волжский Волгоградской области

1. Общие положения

1.1. Настоящий Порядок определяет принципы разграничения доступа пользователей к обрабатываемой информации в муниципальном автономном учреждении «Парк культуры и отдыха «Волжский» городского округа - город Волжский Волгоградской области (далее МАУ «ПКиО «Волжский»).

1.2. Разграничение доступа пользователей к обрабатываемой информации в МАУ «ПКиО «Волжский» определяется идентификацией и аутентификацией пользователей и может быть:

- физическим;
- информационным.

2. Физическое разграничение доступа

2.1. Под физическим разграничением доступа понимаются физические преграды, ограничивающие несанкционированный доступ в здания и помещения учреждения.

2.2. Для аутентификации пользователя используется охранно-пропускной пункт.

2.3. Пользователям запрещается:

- проникать в здания с входов для технического персонала, окон первых этажей;
- проникать в помещения, допуск в которые не предусмотрен.

3. Информационное разграничение доступа

3.1. Под информационным разграничением доступа понимается авторизация пользователей на объекте вычислительной техники (далее ОВТ) под своей учетной записью.

3.2. В качестве идентификатора пользователя выступает уникальный пароль. присвоенный пользователю ответственным за обеспечение информационной безопасности учреждения.

3.3. Для аутентификации пользователя необходимо при включении ОВТ ввести указанный уникальный пароль в поле ввода.

3.4. Учетная запись пользователя должна быть с минимальным набором полномочий, достаточных для выполнения пользователем своих трудовых обязанностей.

3.5. При аутентификации пользователь не должен обладать полномочиями. достаточными для:

- изменения и (или) удаления системных файлов;
- остановки или управления антивирусным программным обеспечением, иными средствами защиты информации;
- установки стороннего программного обеспечения;
- удаления установленного программного обеспечения;
- подключения сторонних аппаратных устройств.

3.6. Пользователям запрещается:

- выполнять на ОВТ любую деятельность, кроме рабочей;

- передавать уникальный пароль третьим лицам и другим пользователям;
- находить уязвимости системы защиты и пытаться их взламывать;
- подключать сторонние аппаратные устройства и программное обеспечение.

4. Ответственность

Каждый сотрудник МАУ «ПКиО «Волжский» несет персональную ответственность за несоблюдение настоящего Порядка.

Директор А.Г. Минаев

Приложение8
к приказу МАУ «ПКиО «Волжский»
от 04 05 22 № 23

Положение
о подключении и использовании ресурсов информационно-телекоммуникационной сети Интернет в муниципальном автономном учреждении «Парк культуры и отдыха «Волжский» городского округа - город Волжский Волгоградской области

1. Общие положения

1. Настоящее Положение определяет и регулирует правила безопасного подключения локально-вычислительной сети, объектов вычислительной техники, иных информационных ресурсов муниципального автономного учреждения «Парк культуры и отдыха «Волжский» городского округа - город Волжский Волгоградской области (далее МАУ «ПКиО «Волжский») к информационно-телекоммуникационной сети Интернет.

1.1. В настоящем Положении описан порядок работы пользователей в информационно-телекоммуникационной сети Интернет, права и обязанности пользователей.

2. Правила подключения к информационно-телекоммуникационной сети Интернет

2.1. Подключение информационных систем, объектов вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети Интернет (далее сеть Интернет), допускается только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.

2.2. Подключение информационных систем, объектов вычислительной техники, применяемых для хранения конфиденциальной информации, не составляющей государственную тайну, общедоступной информации в МАУ «ПКиО «Волжский». осуществляется только с использованием средств защиты информации, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.

1.1. Подключение к сети Интернет осуществляется и регулируется ответственным за обеспечение информационной безопасности учреждения.

2.3. Подключение к сети Интернет ограничено. Пользователям не должны быть доступны следующие информационные ресурсы:

- запрещенных в Российской Федерации движений и организаций;
- социальные сети, мессенджеры и видеохосгинги;
- материалы эротико-порнографического содержания;
- анонимайзеры и сайты с подменой IP-адреса (местонахождения);
- почтовые сервисы, за исключением корпоративной электронной почты.

3. Контроль доступа к сети Интернет

3.1. В целях обеспечения информационной безопасности информационных ресурсов МАУ «ПКиО «Волжский» ответственный за обеспечение информационной безопасности учреждения:

- осуществляет выборочные и (или) полные проверки объектов вычислительной техники, сетевого или коммутационного оборудования;
- обеспечивает работоспособность (настройка, обновление, функционирование) антивирусного программного обеспечения, межсетевого экранирования, иных средств защиты информации, необходимых для безопасного подключения МАУ «ПКиО «Волжский» и ее ресурсов к сети Интернет;
- осуществляет мониторинг локально-вычислительной сети на предмет несанкционированного доступа со стороны пользователей сети Интернет, предпринимает соответствующие мероприятия в случае обнаружения такого доступа;
- докладывает директору учреждения о любых нарушениях, связанных с исполнением настоящего Положения;
- осуществляет сбор статистики посещения пользователями информационных ресурсов в сети Интернет;
- проводит методическую консультацию пользователей в рамках своих компетенций.

4. Права и обязанности пользователей

4.1. Доступ к информационным ресурсам сети Интернет предоставляется сотрудникам МАУ «ПКиО «Волжский» для выполнения ими прямых должностных обязанностей, а именно для:

- доступа к ресурсам сети Интернет в рамках должностных обязанностей сотрудников МАУ «ПКиО «Волжский»;
- доступа к специализированным базам данных (правовые базы и другие);
- контактов с руководителями и сотрудниками сторонних организаций;
- повышения квалификации работников, необходимой для выполнения ими своих должностных обязанностей;
- поиска и сбора информации по управленческим, производственным, финансовым, юридическим вопросам, если эти вопросы напрямую связаны с выполнением работниками своих должностных обязанностей.

4.2. Пользователям категорически запрещается:

- допускать к информационной системе, объекту вычислительной техники лиц, не являющихся сотрудниками МАУ «ПКиО «Волжский», либо сотрудников, не имеющих достаточных полномочий для работы в соответствующих информационной системе, объекте вычислительной техники;
- подключать объекты вычислительной техники к сети Интернет по неслужебным каналам связи (смартфон, модем и пр.);
- загружать, устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления программного обеспечения, если эта работа не входит в его должностные обязанности;
- использовать служебные мощности для нерабочих целей (посещать веб-сайты, не относящиеся к рабочей деятельности, использовать онлайн-майнеры и пр.);
- осуществлять противоправные действия по отношению к локально-вычислительной сети МАУ «ПКиО «Волжский», сотрудников МАУ «ПКиО «Волжский», третьих лиц (рассылка вирусов, DOS-атаки, SQL-инъекции и пр.);
- использовать неслужебные сервисы для обмена конфиденциальной информацией между сотрудниками администрации;
- совершать иные действия, противоречащие законодательству Российской Федерации.

5. Ответственность

За нарушение требований настоящего Положения пользователи и ответственный за обеспечение информационной безопасности учреждения несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

Директор А.Г. Минаев