УТВЕРЖДАЮ

Директор ГБУК КК
«ККУНБ им. А.С.Пушкина»
_____В.В. Гончарова
«18» марта 2021 года

Политика информационной безопасности государственного бюджетного учреждения культуры Краснодарского края «Краснодарская краевая универсальная научная библиотека им. А.С. Пушкина»

1. Общие положения

Информация является ценным и важным ресурсом ГБУК КК «ККУНБ им. А.С. Пушкина» (далее – учреждение). Настоящая политика информационной безопасности (далее - Политика) предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной (смешанной) обработки данных в учреждении.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник учреждения, при этом первоочередной задачей является обеспечение безопасности всех информационных активов учреждения.

В настоящей Политике терминология представлена в соответствии с ГОСТ Р ИСО/МЭК 27002-2012.

Политика разработана в соответствии с нормативными актами:

1.Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 09.03.2021) "Об информации, информационных технологиях и о защите информации".
2.Приказ министерства культуры Краснодарского края от 25.02.2020 №83 "О мерах антитеррористической защищенности государственных учреждений, подведомственных министерству культуры Краснодарского края" (пункт 16).
3.ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности" (утв. и введен в действие Приказом Росстандарта от 24.09.2012 № 423-ст).

1. Цель и назначение настоящей Политики

1.1.Целями настоящей Политики являются:

- сохранение конфиденциальности информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам учреждения для поддержки деятельности;
- защита целостности деловой информации с целью поддержания возможности учреждения по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомленности сотрудников в области рисков, связанных с информационными ресурсами учреждения;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в учреждении.

В Политике изложен общий подход учреждения к организации информационной безопасности. Руководители подразделений учреждения должны обеспечить регулярный контроль за соблюдением положений настоящей Политики. Кроме того, должна быть организована периодическая проверка соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки.

1.2. Область применения настоящей Политики

Требования настоящей Политики распространяются на всю информацию и ресурсы обработки информации учреждения. Соблюдение настоящей Политики обязательно для всех сотрудников (как постоянных, так и временных). В договорах с третьими лицами, получающими доступ к информации учреждения, должна быть оговорена обязанность третьего лица по соблюдению требований настоящей Политики.

1.3.Объектами информационной безопасности являются:

защита данных и конфиденциальность персональных данных;

защита документов учреждения;

иная информация, полученная в результате делопроизводства, заключения контрактов, договоров, соглашений с контрагентами, выполнения требований закона и контролирующих органов.

2. Требования и рекомендации

2.1. Ответственность за обеспечение сохранности и достоверности информации, используемой или производимой в конкретном отделе учреждения возлагается на заведующего (начальника) отдела и непосредственного исполнителя (пользователя информацией).

2.1.1.Безопасность, связанная с персоналом

Учреждение тщательно проверяет всех кандидатов на постоянную работу, подрядчиков и представителей третьей стороны, согласно соответствующим законам, инструкциям и правилам этики, пропорционально значимости (классификации) информации, к которой будет осуществляться доступ, и предполагаемым рискам. Администрация учреждения обеспечивает безопасность конфиденциальной информации (персональных данных) на протяжении всего времени занятости сотрудника в организации.
Отдел кадров, как правило, отвечает за общий процесс приема на работу и прекращения занятости и действует совместно с непосредственным руководителем (заведующим отдела) увольняемого лица, чтобы обеспечить управление аспектами безопасности значимых процедур.
Если увольняемый сотрудник знал пароли к учетным записям, остающимся активными, то эти пароли должны быть изменены после прекращения занятости, договора или соглашения, или при смене занятости.

2.2. Контроль доступа к информационным системам

2.2.1. Общие положения
Все работы в пределах помещений учреждения выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в учреждении.
Внос в помещения учреждения личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы производится только при согласовании с администрацией.
Руководители подразделений (заведующие отделами) должны периодически пересматривать права доступа своих сотрудников к соответствующим информационным ресурсам в связи с увольнением и поступлением на работу новых сотрудников, назначением на новые должности, появлением новых информационных ресурсов, требующих защиты.
В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.
Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.
В процессе своей работы сотрудники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 15 минут (при необходимости или выполнении работ, связанных с обработкой конфиденциальной информации или с грифом "Для служебного пользования").

2.2.2. Доступ третьих лиц к системам учреждения

Доступ третьих лиц к информационным системам учреждения должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам учреждения должен быть четко определен, контролируем и защищен (при работе с зашифрованными данными, передаче информации по защищенным каналам связи). Необходимость защиты информации должна быть указана при заключении контракта, договора, соглашения, если такая защита требуется.

2.2.3. Удаленный доступ

Сотрудникам, работающим за пределами учреждения с использованием компьютера, не принадлежащего учреждению, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ, без согласования с администрацией учреждения.

Все компьютеры, подключаемые посредством удаленного доступа к информационной сети учреждения, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

2.2.4. Доступ к сети Интернет

Доступ к сети Интернет в учреждении обеспечивается только в служебных целях и не может использоваться для незаконной деятельности.

Рекомендованные правила:

сотрудникам учреждения разрешается использовать сеть Интернет только в служебных целях;

запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

работа сотрудников учреждения с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи конфиденциальной информации учреждения или имеющей статус "Для служебного пользования" в сеть Интернет;

сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем учреждению, в личных целях;

сотрудники учреждения перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

запрещен доступ в Интернет через сеть учреждения для всех лиц, не являющихся сотрудниками учреждения.

2.3. Защита оборудования

Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация

учреждения. В учреждении обеспечивается пропускной режим. О появлении посторонних лиц в учреждении любой сотрудник обязан сообщить в администрацию. Посторонние лица (не сотрудники учреждения) перемещаются внутри учреждения только в сопровождении сотрудников учреждения. Пользователи могут самостоятельно перемещаться только в отделы обслуживания.

Сотрудникам запрещается самостоятельно переставлять оборудование, изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят авторизованные специалисты учреждения.

2.3.1. Аппаратное обеспечение

Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей Политики вместе именуются «компьютерное оборудование». Компьютерное оборудование, предоставленное учреждением, является ее собственностью и предназначено для использования исключительно в производственных целях.

Для установки режимов защиты пользователь должен обратиться в отдел автоматизации. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

При записи какой-либо информации на носитель для передачи его контрагентам или партнерам необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

2.3.2. Программное обеспечение

Все программное обеспечение, установленное на предоставленном учреждением компьютерном оборудовании, является собственностью учреждения и должно использоваться исключительно в служебных целях.

Сотрудникам, за исключением сотрудников отдела автоматизации или по разрешению администрации, запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, программное обеспечение, не имеющее отношения к их трудовой деятельности.

Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты.

Сотрудники учреждения не должны:

блокировать антивирусное программное обеспечение;

устанавливать другое антивирусное программное обеспечение;

изменять настройки и конфигурацию антивирусного программного обеспечения.

2.4. Правила пользования электронной почтой

Электронные сообщения (удаленные или не удаленные) могут быть доступны или получены государственными органами, или контрагентами для их использования в качестве доказательств в процессе судебного разбирательства или при осуществлении договорных обязательств. Поэтому содержание электронных сообщений должно строго соответствовать этики служебного поведения учреждения.

Сотрудникам запрещается направлять партнерам конфиденциальную информацию учреждения по электронной почте без использования систем шифрования. Строго конфиденциальная информация учреждения, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

Сотрудникам учреждения запрещается использовать публичные почтовые ящики электронной почты для осуществления какого-либо из видов корпоративной деятельности.

Сотрудники учреждения для обмена документами с контрагентами должны использовать только свой официальный адрес электронной почты.

Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

Ниже перечислены недопустимые действия и случаи использования электронной почты:

рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;

рассылка рекламных материалов, не связанных с деятельностью учреждения;

подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;

поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);

пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит корпоративным стандартам в области этики.

Ко всем исходящим сообщениям, направляемым внешним пользователям, пользователь может добавлять уведомление о конфиденциальности.

Вложения, отправляемые вместе с сообщениями, следует использовать с должной осторожностью. Во вложениях всегда должна указываться дата их подготовки, и они должны оформляться в соответствии с установленными в учреждении процедурами документооборота.

2.5. Сообщение об инцидентах информационной безопасности, реагирование и отчетность

Все сотрудники должны быть осведомлены о своей обязанности сообщать специалистам отдела автоматизации или администрации об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности. На основании обнаружения факта или угрозы нарушения информационной безопасности делается запись в Контрольный Журнал регистрации событий, связанных с информационной безопасностью.

Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

проинформировать специалистов отдела автоматизации;

не пользоваться и не выключать зараженный компьютер, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование специалистами отдела автоматизации.

2.6. Физическая защита и сохранность данных

2.6.1. В учреждении установлены физические барьеры (турникеты, рамки с металлодетекторами), предотвращающие неавторизованный физический доступ в помещение учреждения, доступ разрешен только авторизованному персоналу.

В учреждении выделена зона регистрации пользователей и посетителей.

Все аварийные выходы на случай пожара оборудованы аварийной сигнализацией, которая регулярно подвергается мониторингу и тестированию.

Использование фото-, видео-, аудио- и другого записывающего оборудования, например камер, имеющихся в мобильных устройствах, в помещении учреждения запрещено. Разрешается производить видеосъемку работникам СМИ только по согласованию с администрацией учреждения.

2.6.2. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на сотрудниках, использующих данное рабочее оборудование. Необходимо регулярно делать резервные копии всех основных служебных данных.

Только специалисты отдела автоматизации на основании заявок руководителей подразделений могут создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

2.6.3. Договоры с третьей стороной, привлеченной к доступу, обработке, передаче или управлению информацией или средствами обработки информации организации, или к дополнению продуктов или услуг к средствам обработки информации, должны охватывать все соответствующие требования безопасности. Например, включение в контракт с целью удовлетворения установленных требований безопасности политики информационной безопасности контрагента.

2.6.4.Учреждение проводит ежегодную инвентаризацию наиболее важных материальных и нематериальных активов.