14.03.2019 г. государственное автономное учреждение культуры Ростовской области «Ростовская областная филармония» (ГАУК РО «Ростоблфилармония») переименовано в государственное автономное учреждение культуры Ростовской области «Ростовская государственая филармония» (ГАУК РО «Ростгосфилармония»)

Приказ от 04.03.2019 г. № 23/01-01/85 Министерства культуры Ростовской области

УТВЕРЖДАЮ
Генеральный директор
ГАУК РО «Ростоблфилармония»
_____ О.И. Яковлева
«22» 06 2016 г

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГАУК РО «Ростоблфилармония»

1. Вводные положения

1.1. Введение

Политика информационной безопасности ГАУК РО «Ростоблфилармония» определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется ГАУК РО «Ростоблфилармония» в своей деятельности.

1.2. Цели

Основными целями политики информационной безопасности ГАУК РО «Ростоблфилармония» являются защита информации учреждения и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в его Уставе.

Общее руководство обеспечением информационной безопасности (далее – ИБ) в филармонии осуществляет генеральный директор ГАУК РО «Ростоблфилармония». Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет ответственное лицо, назначенное приказом Генерального директора.

Сотрудники учреждения обязаны соблюдать порядок обращения с защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

1.3. Задачи

Политика информационной безопасности ГАУК РО «Ростоблфилармония» направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Для противодействия угрозам информационной безопасности в ГАУК РО «Ростоблфилармония» составляется прогностическая модель предполагаемых угроз и модель нарушителя.

Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная система управления ИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для ГАУК РО «Ростоблфилармония». Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и

организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

Задачами настоящей политики являются:

– описание организации системы управления информационной безопасностью в ГАУК РО «Ростоблфилармония»;

– определение Политик информационной безопасности ГАУК РО «Ростоблфилармония», а именно:

– Политика реализации антивирусной защиты;

– Политика предоставления доступа к информационному ресурсу;

– Политика использования информационного ресурса в рамках существующих информационных систем;

– Политика использования паролей;

– Политика защиты АРМ;

– Политика конфиденциального делопроизводства;

– определение порядка сопровождения ИС ГАУК РО «Ростоблфилармония».

1.4. Область действия

Настоящая Политика обязательна для исполнения всеми сотрудниками и должностными лицами ГАУК РО «Ростоблфилармония». Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах ГАУК РО «Ростоблфилармония», а также в договорах.

1.5. Период действия и порядок внесения изменений

Актуализация политики информационной безопасности производится в обязательном порядке в следующих случаях:

– при изменении политики РФ в области информационной безопасности, указов и законов РФ в области защиты информации;

– при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности ГАУК РО «Ростоблфилармония»;

– при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб ГАУК РО «Ростоблфилармония».

2. Термины и определения

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Анализ риска – систематическое использование информации для определения источников и оценки риска.

Аудит информационной безопасности – процесс проверки выполнения установленных требований по обеспечению информационной безопасности.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

Внутренняя сеть – внутренний участок корпоративной сети, отделенный от внешней сети (сети Интернет) и DMZ межсетевым экраном.

Демилитаризованная зона (DMZ) – участок корпоративной сети, расположенный между внешним МЭ и внешним маршрутизатором, используемым для подключения корпоративной сети к сети телекоммуникационных провайдеров (сети Интернет). В DMZ размещаются серверы, используемые для взаимодействия и предоставления сетевых сервисов внешним пользователям корпоративной сети, а также серверы, которые по соображениям информационной безопасности не целесообразно размещать во внутренней сети ГАУК РО «Ростоблфилармония».

Доступ к информации – возможность получения информации и ее использования.

Доступность информации – состояние информации, характеризуемое способностью обеспечивать беспрепятственный доступ к информации субъектов имеющих на это полномочия.

Защищенный канал передачи данных – логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных (средствами VPN), либо путем их физической изоляции и размещения на охраняемой территории.

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов филармонии в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов.

Информационная среда – совокупность информационно-телекоммуникационной системы ГАУК РО «Ростоблфилармония», процессов, источников и потребителей информации, обслуживающего персонала и пользователей информационных систем, обеспечивающего автоматизацию производственных процессов ГАУК РО «Ростоблфилармония».

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения производственных задач подразделений филармонии. В ГАУК РО «Ростоблфилармония» используются различные типы информационных систем для решения производственных, управленческих, учетных и других задач.

Информационно-телекоммуникационная система – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники, а также информационные системы, обеспечивающие автоматизацию процессов ГАУК РО «Ростоблфилармония», и средства защиты информации.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационные активы – информационные системы, информационные средства, информационные ресурсы.

Информационные средства – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий, используемая в производственных - процессах ГАУК РО «Ростоблфилармония».

Инфраструктура открытых ключей (ИОК, PKI) – технологическая инфраструктура и сервисы, обеспечивающие безопасность информационных и коммуникационных систем на основе использования криптографических алгоритмов и сертификатов ключей подписей.

Инцидент информационной безопасности – действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов учреждения.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

Код аутентификации электронного сообщения – данные, используемые для установления подлинности и контроля целостности электронного сообщения.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность – доступ к информации только авторизованных пользователей.

Корпоративная сеть – объединение информационных систем, компьютерного, телекоммуникационного и офисного оборудования всех подразделений ГАУК РО «Ростоблфилармония», посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений ГАУК РО «Ростоблфилармония», привести к причинению ГАУК РО «Ростоблфилармония» материального или иного вида ущерба.

Локальная вычислительная сеть (ЛВС) – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах здания.

Межсетевой экран (МЭ) – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав корпоративной сети, а также между корпоративной сетью и внешними сетями (сетью Интернет).

Менеджмент риска – скоординированные действия по руководству и управлению учреждением в отношении риска.

Мониторинг информационной безопасности – постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы учреждения, информационные услуги учреждения и пр.

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Обработка риска – процесс выбора и осуществления мер по модификации риска.

Операционная система – системная программа, осуществляющая взаимодействие пользователя и прикладных программ с аппаратной частью ЭВМ.

Остаточный риск – риск, остающийся после обработки риска.

Оценивание риска – процесс сравнения оцененного риска с данными критериями риска для определения значимости риска.

Оценка риска – общий процесс анализа риска и оценивания риска.

Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

Периметральное средство защиты информации (СЗИ) – шлюз информационной безопасности, обеспечивающий межсетевое экранирование и защиту данных пересылаемых по открытым каналам связи (шифрование), а так же фильтрацию вредоносного ПО и блокирование внешних атак.

Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в учреждении для обеспечения его информационной безопасности.

Пользователь ЛВС – сотрудник ГАУК РО «Ростоблфилармония» (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в корпоративной сети в установленном порядке и получивший права на доступ к ресурсам корпоративной сети в соответствии со своими функциональными обязанностями.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Сервер – выделенный компьютер, имеющий разделяемые ресурсы, выполняющий определенный перечень задач и предоставляющий пользователям ЛВС ряд сервисов.

Средства криптографической защиты информации – средства шифрования, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Структурное подразделение – структурное подразделение учреждения с самостоятельными функциями, задачами и ответственностью.

Угрозы информационным данным – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Управление информационной безопасностью – совокупность целенаправленных действий, осуществляемых в рамках политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности учреждения при реализации угроз в информационной сфере.

Целостность информации – состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца ключа подписи, а также установить отсутствие искажения информации в электронном документе.

VPN (VIRTUAL PRIVATE NETWORK) – «Виртуальная частная сеть»: технология и организация систематической удаленной связи между выбранными группами узлов в крупных распределенных сетях.

3. Политика информационной безопасности ГАУК РО «Ростоблфилармония».

3.1. Назначение политики информационной безопасности

Политика информационной безопасности ГАУК РО «Ростоблфилармония» – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в ГАУК РО «Ростоблфилармония».

Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика информационной безопасности относится к административным мерам обеспечения информационной безопасности и определяет стратегию ГАУК РО «Ростоблфилармония» в области ИБ.

Политика информационной безопасности (далее, ПБ) регламентирует эффективную работу средств защиты информации. Она охватывает все особенности процесса обработки информации, определяя поведение информационной системы (далее – ИС) и ее пользователей в различных ситуациях. Политика информационной безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политику, должны быть утверждены руководителем учреждения.

3.2. Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются следующие:

– Постоянный и всесторонний анализ информационного пространства филармонии с целью выявления уязвимостей информационных активов.

– Своевременное обнаружение проблем, потенциально способных повлиять на ИБ филармонии, корректировка моделей угроз и нарушителя.

– Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей филармонии, а также повышать трудоемкость технологических процессов обработки информации.

– Контроль эффективности принимаемых защитных мер.

– Персонификация и адекватное разделение ролей и ответственности между сотрудниками учреждения, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

3.3. Соответствие ПБ действующему законодательству

Правовую основу политики составляют Конституция Российской Федерации, законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, ГАУК РО «Ростоблфилармония» и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

3.4. Ответственность за реализацию политик информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт лицо, назначенное приказом Генерального директора.

Ответственность в части, касающейся исполнения правил политики, – на каждого сотрудника ГАУК РО «Ростоблфилармония», согласно должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

3.5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Обучение сотрудников ГАУК РО «Ростоблфилармония» правилам обращения с конфиденциальной информацией проводится путем самостоятельного изучения

сотрудниками внутренних нормативных документов филармонии в области защиты персональных данных под роспись в документе.

Допуск персонала к работе с информационными ресурсами ГАУК РО «Ростоблфилармония» осуществляется только после его ознакомления с настоящими документами, а также после ознакомления пользователей с «Инструкцией пользователя по соблюдению режима информационной безопасности в ГАУК РО «Ростоблфилармония», а так же иными документами. Согласие на соблюдение правил и требований по защите информации подтверждается подписями сотрудников в «Инструкции».

Допуск персонала к работе с конфиденциальной информацией ГАУК РО «Ростоблфилармония» осуществляется после ознакомления с «Инструкцией пользователя по соблюдению режима информационной безопасности в ГАУК РО «Ростоблфилармония». Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками ГАУК РО «Ростоблфилармония», определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

3.6. Защищаемые информационные ресурсы ГАУК РО «Ростоблфилармония»

Подходы к решению проблемы защиты информации в ГАУК РО «Ростоблфилармония», в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования производственных процессов ГАУК РО «Ростоблфилармония».

Для этого в ГАУК РО «Ростоблфилармония» выполняются следующие мероприятия:

- определяется порядок работы с документами, содержащими персональные данные;
- устанавливается круг лиц и порядок доступа к подобной информации;
- вырабатываются меры по контролю обращения с документами, содержащими персональные данные;
- разрабатывается инструкция по обращению с персональными данными, с которой работники знакомятся под роспись.

«Обязательство о неразглашении персональных данных работников» подписывается при заключении трудового договора, который подписывается сотрудниками учреждения, допущенными к обработке персональных данных, при приеме на работу в ГАУК РО «Ростоблфилармония». Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых ГАУК РО «Ростоблфилармония» с другими организациями.

Согласно Ст.86 п.7 Трудового кодекса РФ защита персональных данных сотрудника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

Согласно Ст.88 Трудового кодекса РФ при передаче персональных данных сотрудника работодатель должен соблюдать следующие требования:

- осуществлять передачу персональных данных сотрудника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым сотрудник должен быть ознакомлен под расписку;
- разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретных функций.

Согласно Ст.90 Трудового кодекса РФ лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника, несут

дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

3.7. Организация системы управления информационной безопасностью (ИБ) ГАУК РО «Ростоблфилармония»

3.7.1. Организация системы управления ИБ

Система управления информационной безопасности ГАУК РО «Ростоблфилармония» – предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности ГАУК РО «Ростоблфилармония»

Для успешного функционирования СУИБ ГАУК РО «Ростоблфилармония» должны быть реализованы следующие процессы:

– определение и уточнение области действия СУИБ и выбор подхода к оценке рисков ИБ.

– определение и уточнение области действия СУИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью ГАУК РО «Ростоблфилармония», а также оценки репутационных и правовых рисков деятельности ГАУК РО «Ростоблфилармония»;

– анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов и производственных процессов.

– выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ.

– принятие руководством ГАУК РО «Ростоблфилармония» остаточных рисков и решения о реализации и эксплуатации/совершенствовании СУИБ. Остаточные риски ИБ должны быть соотнесены с рисками деятельности ГАУК РО «Ростоблфилармония» и оценено их влияние на достижение целей деятельности ГАУК РО «Ростоблфилармония».

3.7.2. Реализация системы управления ИБ

В системе управления ИБ должны быть реализованы следующие процессы:

– разработка плана обработки рисков ИБ;

– реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СУИБ;

– реализация программ по обучению и осведомленности ИБ;

– обнаружение и реагирование на инциденты безопасности;

– обеспечение непрерывности деятельности и восстановления после прерываний.

На этапе планирования определяется политика и методология управления рисками, а также выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, определение допустимого уровня остаточных рисков.

На этапе реализации производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации. ГАУК РО «Ростоблфилармония» принимается одно из четырех решений по каждому идентифицированному риску: проигнорировать, избежать, передать внешней стороне, либо минимизировать. После этого разрабатывается и внедряется план обработки рисков.

На этапе проверки отслеживается функционирование механизмов контроля, контролируются изменения факторов риска (активов, угроз, уязвимостей), проводится аудит и выполняются различные контролирующие процедуры.

На этапе действия по результатам непрерывного мониторинга и проводимых проверок, выполняются необходимые корректирующие действия, которые могут включать в себя, в частности, переоценку величины рисков, корректировку политики и методологии управления рисками, а также плана обработки рисков.

3.7.3. Методы оценивания информационных рисков

Оценка информационных рисков ГАУК РО «Ростоблфилармония» выполняется по следующим основным этапам:

– идентификация и оценка информационных ресурсов, значимых для работы ГАУК РО «Ростоблфилармония»;
– оценивание возможных угроз;
– оценивание существующих уязвимостей;
– оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые для производственного процесса уязвимые информационные ресурсы ГАУК РО «Ростоблфилармония» подвергаются риску, если по отношению к ним существуют какие-либо угрозы.

При этом информационные риски зависят от:

– показателей ценности информационных ресурсов;
– вероятности реализации угроз для ресурсов;
– эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности филармонии.

При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды.

Возможность реализации угрозы оценивается вероятностью ее реализации в течение заданного отрезка времени для некоторого ресурса ГАУК РО «Ростоблфилармония».

При этом вероятность того, что угроза реализуется, определяется следующими основными показателями:

– привлекательностью ресурса, используется при рассмотрении угрозы от умышленного воздействия со стороны человека;
– возможностью использования ресурса для получения дохода, также используется при рассмотрении угрозы от умышленного воздействия со стороны человека;
– техническими возможностями реализации угрозы, используется при умышленном воздействии со стороны человека;
– степенью легкости, с которой уязвимость может быть использована.

3.8. Политики информационной безопасности

3.8.1. Политика предоставления доступа к информационному ресурсу

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к информационным ресурсам ГАУК РО «Ростоблфилармония».

К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей политикой.

3.8.2. Политика использования паролей

Настоящая политика определяет основные правила обращения с паролями, используемыми для доступа к информационным активам ГАУК РО «Ростоблфилармония».

Положения политики закрепляются в «Инструкции пользователя по соблюдению режима информационной безопасности».

3.8.3. Политика реализации антивирусной защиты

Настоящая Политика определяет основные правила для реализации антивирусной защиты в ГАУК РО «Ростоблфилармония».

Положения политики закрепляются в «Инструкции пользователя по соблюдению режима информационной безопасности».

3.8.4. Политика защиты АРМ

Настоящая Политика определяет основные правила и требования по защите конфиденциальной информации ГАУК РО «Ростоблфилармония» от неавторизованного доступа, утраты или модификации.

Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

Сотрудники получают доступ к ресурсам вычислительной сети после ознакомления с «Инструкцией пользователя по соблюдению режима информационной безопасности».

Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только ответственному лицу. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к корпоративной информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к системному администратору, а все обращения должны регистрироваться.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных сетевых ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.

Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.

АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками ГАУК РО «Ростоблфилармония». Запрещается использование указанных АРМ другими пользователями без согласования с непосредственным начальником. При передаче указанного АРМ другому пользователю, должна производится гарантированная очистка диска (форматирование).

Системный администратор вправе отказать в устранении проблемы, вызванной наличием на рабочем месте программного обеспечения или оборудования, установленного или настроенного пользователем в обход действующей процедуры.

3.9. Порядок сопровождения ИС (информационных систем) ГАУК РО «Ростоблфилармония»

Обеспечение информационной безопасности информационных систем на стадиях жизненного цикла ИБ ИС должна обеспечиваться на всех стадиях жизненного цикла (ЖЦ) ИС, автоматизирующих технологические процессы, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации). Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводится при участии администратора информационной безопасности и системного администратора. Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться.

При разработке ИС необходимо придерживаться требований и методических указаний, определенных «Стандартами информационной технологии».

На стадиях, связанных с разработкой ИС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

- неверной формулировки требований к ИС;
- выбора неадекватной модели ИС, в том числе неадекватного выбора процессов и вовлеченных в них участников;
- принятия неверных проектных решений;
- внесения разработчиком дефектов на уровне архитектурных решений;
- внесения разработчиком недокументированных возможностей в ИС;
- неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к ИС;
- разработки некачественной документации;
- сборки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований;
- неверного конфигурирования ИС;
- приемки ИС, не отвечающей требованиям заказчика;
- внесения недокументированных возможностей в ИС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

Привлекаемые для разработки и (или) производства средств и систем защиты ИС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ.

При приобретении готовых ИС и их компонентов разработчиком должна быть предоставлена документация, содержащая, в том числе, описание защитных мер, предпринятых разработчиком в отношении угроз информационной безопасности.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком ИС и их компонентов относительно безопасности разработки, безопасности поставки, эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, оценки уязвимости. Данная документация может быть представлена в рамках декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки.

На стадии эксплуатации должна быть обеспечена защита от следующих угроз:

– умышленное несанкционированное раскрытие, модификация или уничтожение информации;
– неумышленная модификация или уничтожение информации;
– недоставка или ошибочная доставка информации;
– отказ в обслуживании или ухудшение обслуживания.

Кроме этого, актуальной является угроза отказа от авторства сообщения. На стадии сопровождения должна быть обеспечена защита от угроз:

– внесения изменений в ИС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей;
– невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС.

На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб ГАУК РО «Ростоблфилармония», и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС или с внешних носителей.

Требования ИБ должны включаться во все договора и контракты на проведение работ или оказание услуг.

3.9.1. Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений политик информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений информационной безопасности в ГАУК РО «Ростоблфилармония» и проведение разъяснительной работы по информационной безопасности среди пользователей.

Задача предупреждения в ИС ГАУК РО «Ростоблфилармония» возможных нарушений информационной безопасности решается по мере наступления следующих событий:

– включение в состав ИС ГАУК РО «Ростоблфилармония» новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в ИС ГАУК РО «Ростоблфилармония»;
– изменение конфигурации программных и технических средств ИС ГАУК РО «Ростоблфилармония» (изменение конфигурации программного обеспечения рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в ИС ГАУК РО «Ростоблфилармония»;
– при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения технических средств, используемых в ИС ГАУК РО «Ростоблфилармония».

Администратор информационной безопасности (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения относительно ИС ГАУК РО «Ростоблфилармония».

Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, общественных объединений и других организаций, специализирующихся в области защиты информации.

Администратор информационной безопасности (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) организовывает периодическую проверку ИС ГАУК РО «Ростоблфилармония» путем моделирования возможных попыток осуществления несанкционированного доступа к защищаемым информационным ресурсам.

Для решения задач контроля защищенности ИС используются инструментальные средства для тестирования реализованных средств и функций защиты. По результатам профилактических работ необходимо сделать соответствующие записи в Журнале проверки исправности и технического обслуживания.

Плановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников ГАУК РО «Ростоблфилармония» по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в ГАУК РО «Ростоблфилармония», проводится ответственным лицом ежеквартально.

Внеплановая разъяснительная работа по правилам настоящих политик, а также инструктаж сотрудников ГАУК РО «Ростоблфилармония» по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в ГАУК РО «Ростоблфилармония», проводится при пересмотре настоящих политик, при возникновении инцидента нарушения правил настоящих политик.

Прием на работу новых сотрудников должен сопровождаться ознакомлением их с правилами и требованиями настоящих политик.

3.9.2. Ликвидация последствий нарушения политик информационной безопасности

Ответственное лицо, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС ГАУК РО «Ростоблфилармония», должны своевременно обнаруживать нарушения информационной безопасности, факты осуществления несанкционированного доступа к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения информационной безопасности или осуществления несанкционированного доступа к защищаемым информационным ресурсам ИС ГАУК РО «Ростоблфилармония» рекомендуется уведомить ответственное лицо и непосредственного начальника, и далее следовать их указаниям.

Действия ответственных лиц при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

– Инструкцией пользователя по соблюдению режима информационной безопасности;

– Политикой информационной безопасности;

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС ГАУК РО «Ростоблфилармония», а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации и причин их последствий.

3.9.3. Ответственность нарушителей ПБ

Ответственность за выполнение правил Политик безопасности несет каждый сотрудник ГАУК РО «Ростоблфилармония» в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политики безопасности ГАУК РО «Ростоблфилармония», могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный ГАУК РО «Ростоблфилармония» в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса РФ).

За умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, сотрудники ГАУК РО «Ростоблфилармония» несут материальную ответственность в полном размере причиненного ущерба (Ст. 243 Трудового кодекса РФ).

4. Регулирующие законодательные нормативные документы

При организации и обеспечении работ по информационной безопасности сотрудники ГАУК РО «Ростоблфилармония» должны руководствоваться следующими законодательными нормативными документами:

- Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.);
- Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов (разработана во исполнение Указа Президента Российской Федерации от 1 июля 1994 г. № 1390 «О совершенствовании информационно-телекоммуникационного обеспечения органов государственной власти и порядке их взаимодействия при реализации государственной политики в сфере информатизации»);
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Указ Президента Российской Федерации от 7 октября 1993 г. № 1607 «О государственной политике в области охраны авторского права и смежных прав»;
- Указ Президента Российской Федерации от 31 декабря 1993 г. № 2334 «О дополнительных гарантиях прав граждан на информацию» (с изменениями от 17 января 1997 г., 1 сентября 2000 г.);
- Указ Президента Российской Федерации от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации» (с изменениями от 26 июля 1995 г., 17 января, 9 июля 1997 г.);
- Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);
- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);