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

Концепция информационной безопасности ГАУК РО «Ростоблфилармония».

Настоящий документ определяет цели, политику в области защиты информации, обозначает задачи, принципы и основные пути обеспечения информационной безопасности (далее - ИБ) ГАУК РО «Ростоблфилармония». Концепция является базовым нормативно-информационным документом и служит основой для:

- создания единой системы правовых, организационных, технических, режимных и иных мер, обеспечивающих защищенность ГАУК РО «Ростоблфилармония» в информационной сфере;
- разработки программ и мероприятий по обеспечению информационной безопасности ГАУК РО «Ростоблфилармония», подготовки локальных нормативных документов.

Организация системы ИБ.

- Генеральный директор – определяет направления и меры по реализации Концепции информационной безопасности;
- Заместители Генерального директора и Генеральный директор – предусматривают выделение средств и координируют работу подразделений по вопросам ИБ; обеспечивают выполнение технических мер ИБ в ГАУК РО «Ростоблфилармония», подбор лучших практик и их внедрение;
- Руководители подразделений – обеспечивают выполнение всеми подчиненными сотрудниками установленных требований ИБ;
- обеспечение ИБ непосредственно на рабочих местах возлагается на сотрудников подразделений.

Ответственность за нарушение требований ИБ.

По степени опасности нарушения ИБ делятся на две группы:

- нарушения, повлекшие за собой наступление нежелательных для ГАУК РО «Ростоблфилармония» последствий (утечку или уничтожение информации);
- нарушения, создавшие предпосылки нежелательных для ГАУК РО «Ростоблфилармония» последствий (угроза уничтожения или утраты информации).

Степень ответственности за нарушение требований локальных нормативных актов в области ИБ определяется исходя из размера ущерба, причиненного ГАУК РО «Ростоблфилармония». Руководители структурных подразделений филармонии несут персональную ответственность за обеспечение ИБ в возглавляемых ими подразделениях.

С Настоящим документом - Концепцией информационной безопасности - руководители всех структурных подразделений ГАУК РО «Ростоблфилармония» обязаны ознакомиться под роспись.

I. ВВЕДЕНИЕ

Информационная безопасность (ИБ) есть защищенность, сохранность информационных ресурсов от случайных, злонамеренных или чрезвычайных внутренних/внешних воздействий и сбоев.

Общая **задача ИБ** состоит в минимизации ущерба, в предсказании и непрерывном предотвращении таких воздействий. ИБ, как важная компонента обеспечения устойчивости работы ГАУК РО «Ростоблфилармония», обеспечивается комплексом организационных, технологических и технических решений и систем. Основы видения и политика ИБ обозначаются настоящим документом, а именно:

- цели и пути создания системы защиты;
- объекты защиты и их характеристика;
- анализ рисков, описывающий финансовые потери, ущерб и потери по другим критериям;
- основные классы и источники угроз ИБ; вероятность угроз и уязвимость ресурсов;
- основные принципы и подходы к построению системы обеспечения ИБ, методы и средства.

II. ЦЕЛИ И ЗАДАЧИ

Целью системы защиты является обеспечение бесперебойной работы аппаратно-программных средств ГАУК РО «Ростоблфилармония», непрерывная поддержка трудовых процессов и документооборота, сохранность и достоверность информационных ресурсов, их защищенность от внутренних и внешних воздействий, а также при чрезвычайных обстоятельствах.

Пути достижения целей можно выделить в несколько направлений:

1. **Организационно-административные мероприятия и регламенты:**
   - определение ответственности за работоспособность и сохранность ресурсов ГАУК РО «Ростоблфилармония» четырех групп сотрудников: **а)** руководящий персонал за выделение средств на приобретение, развертывание систем, привлечение специалистов, развитие и пр.; **б)** конечных пользователей; **в)** сотрудников охраны;
   - обязательное планирование развития информационных ресурсов, технологий и защиты, для достижения устойчивости трудовых процессов и долговременных конкурентных преимуществ;
   - централизация всех мероприятий по закупке, установке аппаратных и программных средств, работе с любыми внешними поставщиками ИТ-услуг;
   - выработка политик пользования информационно-технологическими ресурсами, политик поддержки пользователей, других правовых норм и ответственности по ИБ для всех групп сотрудников (при приеме на работу, на период работы);
   - контроль доступа пользователей к ИТ-ресурсам филармонии.
2. **Надежность, достоверность аппаратного и программного обеспечения:**
   - закупка оборудования и программного обеспечения только известных производителей и продавцов; использование лицензионного программного обеспечения и ресурсов;
   - защита по питанию всего оборудования (ПК, маршрутизаторы и пр.), расположение серверной и коммуникационной техники в приспособленных помещениях с ограниченным доступом и климат контролем, наличие резервных мощностей для наиболее критичных узлов;
   - обязательное пользовательское тестирование, настройка нового оборудования и программного обеспечения перед вводом в эксплуатацию;
   - определение регламентов резервирования данных, периодическое резервное копирование и архивирование данных;
   - периодическое создание образов системного ПО серверов и рабочих станций для быстрого восстановления систем;
   - физическое резервирование наиболее критичных серверов, создание кластеров и пр.
3. **Работа с внешними поставщиками и подрядчиками, аутсорсинг:**
   - определение правил работы с поставщиками услуг и подрядчиками, выделение руководителя проекта со стороны заказчика;

- завершение всех проектных работ комплексным пользовательским тестированием, обучением пользователей и периодом опытной эксплуатации, устранение всех неопределенностей перед внедрением;
- выполнение всех ИТ-работ внутри филармонии только ИТ-специалистом;

4. **Защита от внешних и внутренних воздействий, ограничения прав, криптозащита:**
   - описание мероприятий, направленных на предотвращение утечки информации и несанкционированного доступа;
   - определение правил доступа и работы сотрудников с информационной системой, в т.ч. ответственности по защите от вирусов;
   - выбор технологий передачи информации, использование шифрования (при необходимости);
   - выработка процедур контроля работы информационной системы (протоколирование событий, анализ протоколов, анализ сетевого трафика, анализ работы технических средств);
   - непрерывный мониторинг – использование аппаратно-программных средств защиты (межсетевые экраны, антивирусные программы) и ручного мониторинга;
   - физическая защита и защита помещений, техники и бумажной документации от посторонних органов и лиц.

III. ОБЪЕКТЫ ЗАЩИТЫ

Объектами защиты является вся информационно-технологическая инфраструктура ГАУК РО «Ростоблфилармония», а именно, помещения, компьютерное, периферийное, сетевое оборудование и каналы связи, носители информации и программное обеспечение, данные и информация, функционирование документооборота и трудовых процессов, внутренняя конфиденциальная информация, т.е. все элементы работ, нарушение и доступ к которым ведут к ущербу и потерям.

Подлежащая защите информация может находиться на бумажных носителях, в электронном виде, передаваться в виде электрических сигналов (телефон, телефакс, телекс), присутствовать в виде акустических и вибросигналов в воздушной среде помещений, записываться и воспроизводиться с помощью технических средств (диктофоны, видеомагнитофоны).

Здесь же **ИБ** конкретизируется **в узком понимании** - как комплекс инструментов по защите программно-технических средств. Она должна обеспечивать выполнение трех основных условий:

1. Программно-технические средства должны исправно работать в соответствии с установленной конфигурацией и настройками.
2. На программно-технических средствах должно выполняться только разрешенное программное обеспечение – любые другие программы, вирусы, трояны, даунлоадеры, внешние программы не должны попадать и активизироваться в системе.
3. Доступ к внутренним ресурсам информационной системы должны иметь только авторизованные субъекты согласно своим правам.

IV. ОСНОВНЫЕ КЛАССЫ УГРОЗ

Под **угрозами** ИБ понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

1. Недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств.

2. Утрата сведений, составляющих коммерческую тайну, секреты и иную защищаемую информацию, а также искажение (несанкционированная модификация, подделка) такой информации;
3. Утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.), а также утечка информации по каналам связи и за счет побочных электромагнитных излучений;

Источники угроз ИБ ГАУК РО «Ростоблфилармония» подразделяются на:

- **внутренние**, вызванные действиями сотрудников, авторизованных пользователей информационной системы – доступ и кража конфиденциальной информации, преднамеренное искажение или уничтожение информации в системе, выполнение манипуляций, приводящих к искажению работы системы или ее сбою, несоблюдение элементарных правил безопасной работы с почтой, активными элементами на web-страницах, повреждение данных в результате неосторожных действий и т.д.;
- **внешние**, вызванные внешними воздействиями – сетевые атаки и несанкционированное проникновение в компьютерные сети, вирусы и черви из электронной почты и web-страниц, спам, перехват незашифрованного трафика и т.д.;
- **естественно-технические и чрезвычайные**, вызванные неправильной эксплуатацией оборудования и неправильным хранением данных, кражей или изъятием компьютеров, бумажных и электронных носителей, форс-мажорными обстоятельствами, выходом из строя и пр.

Весь **перечень** источников угроз может быть следующий:

- стихийные бедствия (пожары, наводнения и т.п.);
- технические аварии (внезапное отключение электропитания, протечки и т.п.);
- несанкционированное получение идентификаторов пользователей и их паролей, паролей доступа к общим ресурсам;
- несанкционированная передача защищаемой информации из внутренней (локальной) сети в глобальную сеть Интернет;
- умышленное или неумышленное разглашение защищаемой информации;
- хищение (изъятие) носителей информации или несанкционированное копирование информации;
- хищение (изъятие), физический вывод из строя технических средств;
- посылка в сеть пакетов, нарушающих нормальную работу сети (ложные ARP-запросы и ARP-ответы, перегрузка стеков IP, широковещательные "штормы" и т.д.);
- внедрение программ-троянов, резидентных программ, обеспечивающих получение полного контроля над компьютером; внедрение деструктивных программ – вирусов, сетевых червей и пр.;
- проникновение зловредных программ через Internet (копирование "зараженных" файлов, через апплеты языка Java и объекты ActiveX), электронную почту, гибкие диски, CD-диски;
- получение информации о топологии сети, принципах ее функционирования, характеристической информации сети или участка сети;
- прослушивание сетевого трафика (с целью получения информации о сетевых ресурсах, кешированных паролях, идентификаторах пользователей и пр.) с использованием легальных рабочих станций;
- прослушивание сетевого трафика с использованием нелегальных компьютеров, подключенных к сети физически (локально) или удаленно (Telnet, HTTP);
- внедрение технических и программных средств скрытного съема информации с рабочих станций, средств связи, из помещений ГАУК РО «Ростоблфилармония», в которых обрабатывается защищаемая информация;

- использование специальных методов и технических средств (побочные излучения, наводки по цепям питания, электронные закладки, дистанционное скрытое видео наблюдение или фотографирование, применение подслушивающих устройств, перехват электромагнитных излучений и наводок и т.п.);
- использование для доступа к информации так называемых "люков", "дыр" и "лазеек" и других возможностей обхода механизма разграничения доступа, возникающих вследствие несовершенства общесистемных компонентов программного обеспечения операционных систем, систем управления базами данных и др., неоднозначностями языков программирования, применяемых в автоматизированных системах обработки данных;
- незаконное подключение специальной регистрирующей аппаратуры к устройствам или линиям связи (перехват модемной и факсимильной связи);
- умышленное изменение используемого программного обеспечения с целью несанкционированного сбора защищаемой информации и т.д.

V. ОПРЕДЕЛЕНИЕ РИСКОВ

Негативные последствия угроз:

- финансовые потери, связанные с утечкой или разглашением защищаемой информации (ущерб, связанный с нарушением конфиденциальности);
- финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации и ресурсов (ущерб, связанный с нарушением целостности, доступности информационных ресурсов и т.д.);
- ущерб от дезорганизации деятельности филармонии, простоев и потери, связанные с невозможностью выполнения своих обязательств;
- моральные потери, ущерб репутации филармонии.

Решение о защите конкретных информационно-технологических ресурсов и степени защиты, финансовые и технические решения принимаются исходя из ценности ресурсов по критериям возможных рисков и вероятности угроз.

VI. МЕРЫ ОБЕСПЕЧЕНИЯ ИБ

Общими мерами по обеспечению ИБ ГАУК РО «Ростоблфилармония» являются:

- административно-правовые, организационные и режимные;
- технические, основанные на использовании аппаратно-программных и специальных средств.

Обобщенный перечень **административно-правовых и организационных мер:**

1. Определение правового статуса всех субъектов отношений в информационной среде, установление их ответственности перед ГАУК РО «Ростоблфилармония» через соблюдение нормативных актов, регламентов и политик в сфере ИБ.
2. Разработка правил эксплуатации технических и программных средств (регламентов, порядков) и правил реагирования при нарушении режима безопасности (подозрений на нарушение).
3. Обучение всех сотрудников обеспечению ИБ. Регламентирование работы сотрудников охраны.
4. Аттестация информационных объектов на защищенность (при необходимости).
5. Обеспечение преемственности при разработке технологических и программных решений. Оперативное реагирование (внедрение) на появление новых разработок в области информационных технологий.
6. Обеспечение принципа разграничения доступа: информация должна быть доступна только тем, кому она предназначена и разрешена. Предоставление сотрудникам минимально

достаточных прав по доступу к информации, необходимых для выполнения ими своих функциональных обязанностей.

7. Создание эффективной системы контроля за выполнением требований локальных нормативных актов ИБ. Пользователи информационных ресурсов должны знать о наличии системы контроля и защиты информации.
8. Совершенствование нормативно-правовой базы по работе с конфиденциальной информацией и сведениями внутри филармонии и со сторонними организациями. Разработка Инструкции по ИБ – оперативного документа ежедневного использования, содержащего детальные рабочие инструкции.

Обобщенный перечень **режимных мер:**

1. Определение пропускного и внутриобъектового режима в ГАУК РО «Ростоблфилармония», разграничение доступа и контроль за доступом в выделенные помещения; инструктаж сотрудников охраны;
2. Определение перечня критичной внутренней документации филармонии, мест и сроков ее хранения, порядок доступа и уничтожения.
3. Определение мероприятий и действий при чрезвычайных обстоятельствах для всех подразделений и служб.

Обобщенный перечень **технических мер:**

1. Обеспечение безотказной работы аппаратных средств, резервирование информации.
2. Использование лицензионного программного обеспечения; заказного программного обеспечения, прошедшего этап тестирования и опытной эксплуатации.
3. Использование сертифицированных средств защиты информации для обработки, хранения и передачи конфиденциальной информации, при необходимости использование защищенных соединений с шифрованием, в частности, для удаленных соединений.
4. Проведение комплексной антивирусной защиты.
5. Внедрение в сеть современной системы обнаружения вторжений, мониторинг несанкционированного подключения к информационным ресурсам.
6. Проведение эффективной парольной защиты. Использование единственной системы авторизации пользователей и разграничения прав доступа к ресурсам сети на базе доменной поддержки операционной системы.
7. Проведение контроля состояния программного и информационного обеспечения компьютеров (состава и целостности программного обеспечения, корректности настроек и т.д.) и маршрутизаторов (маршрутных таблиц, фильтров, паролей).
8. Обеспечение резервного копирования.
9. Проведение мониторинга деятельности пользователей (вход-выход в систему, доступ к сетевым ресурсам и пр.), проведение контроля трафика сети на отдельных ее сегментах.
10. Использование внутренних IP-адресов из диапазона, специально выделенного для построения частных сетей. Создание «демилитаризованной зоны» на стыке локальной сети филармонии и внешней сети.
11. Выделение отдельной изолированной подсети для экспериментов по освоению новых технологий и тестированию программного обеспечения, либо использования VMware сред.
12. Определение действий по резервному копированию и защите информации при чрезвычайных обстоятельствах.

Задача обеспечения ИБ должна решаться **системно**. Это означает, что различные средства защиты (аппаратные, программные, физические, организационные и т. д.) должны применяться одновременно, на всех уровнях информационного взаимодействия и под централизованным управлением. При этом компоненты системы должны "знать" о существовании друг друга, взаимодействовать и обеспечивать защиту как от внешних, так и от внутренних угроз.

Арсенал технических методов обеспечения ИБ широк и подбирается после анализа всех рисков:

Уровни безопасности	Применяемые меры безопасности
Периметр	Межсетевой экран, антивирус для шлюзов, VPN, анализаторы контента, IPS (Intrusion Prevention Systems — системы предотвращения вторжений), PKI-решения (Public Key Infrastructure — доверительные отношения с помощью цифровых сертификатов, подписываемых центром сертификации)
Сеть	IDS (Intrusion Detection Systems — системы обнаружения вторжений), межсетевое экранирование, сканнеры оценки уязвимости (Vulnerability-Assessment - VA), аутентификация, управление доступом, управление политиками безопасности, средства контроля содержимого электронной почты, средства контентной фильтрации, защита от утечки по техническим каналам, системы мониторинга событий, защита телефонных систем
Хост	Host IDS, системные сканеры, анализаторы политик безопасности, антивирусы, управление доступом, аутентификация
Приложения	Контроль ввода данных, Host IDS, анализаторы политик безопасности, контроль доступа, аутентификация
Данные	Криптографическая защита (шифрование, подпись), управление доступом, аутентификация