

Государственное бюджетное профессиональное общеобразовательное учреждение
Самарской области
«Сызранский медико-гуманитарный колледж»



Подписан: Касимова Лола Казимовна
DN: О="ГБПОУ ""СМГК"" г.Сызрани",
CN=Касимова Лола Казимовна,
E=medgum@yandex.ru
Основание: я подтверждаю этот
документ своей удостоверяющей
подписью
Местоположение: 00928c62fe5883f88b
Дата: 2026.08.21 09:56:58+04'00'

Утверждаю
Директор ГБПОУ «СМГК»
Л.К. Касимова
Приказ № 169/01-05од
от «21» августа 2026 г.

ПОЛИТИКА информационной безопасности

Введение

Данная Политика информационной безопасности в Государственном бюджетном профессиональном общеобразовательном учреждении «Сызранский медико-гуманитарный колледж (далее – Колледж, Учреждение, ГБПОУ «СМГК») представляет собой фундаментальный документ, определяющий всесторонний подход к обеспечению информационной безопасности во всех сферах деятельности колледжа.

Политика не просто перечисляет правила, а формирует целостное мировоззрение, направленное на защиту ценных информационных активов. Она устанавливает стратегические цели и задачи по защите информации, задавая вектор развития системы управления информационной безопасностью (далее – СУИБ) и описывая принципы ее построения. Успешная реализация уставных задач колледжа напрямую зависит от эффективного обеспечения информационной безопасности, что является одним из ключевых факторов ее жизнеспособности и развития.

Под обеспечением информационной безопасности в рамках данной Политики понимается комплекс мероприятий, направленных на защиту информационных ресурсов колледжа, включая всевозможные данные, программное обеспечение, базы данных, а также всей сопутствующей инфраструктуры: компьютерной техники, сетей связи, систем хранения данных и т.д. Это комплексный подход, охватывающий все автоматизированные системы, телекоммуникационные сети и информационные потоки, которыми владеет и пользуется колледж.

Область действия настоящей Политики распространяется на информационные ресурсы содержащие персональные данные сотрудников, обучающихся и посетителей, на все уровни доступа к информации – от сотрудников до внешних контрагентов, взаимодействующих с информационными системами ГБПОУ «СМГК».

Для сотрудников и обучающихся действие данной политики распространяется на категорию данных «Иные»: - ФИО;

- дата рождения;
- место рождения;
- пол;
- гражданство;
- адрес регистрации;

- адрес проживания;
- дата регистрации по месту жительства;
- контактные телефоны;
- данные документа, удостоверяющего личность;
- наименование органа, выдавшего документ, удостоверяющий личность;
- дата выдачи документа, удостоверяющего личность;
- ИНН;
- СНИЛС;
- реквизиты документа об образовании; – сведения об образовании;

Область действия настоящей Политики распространяется на информационные ресурсы, такие как МИС ЕЦП, Информационная система персональных данных «Ведение бухгалтерского и кадрового учета»: 1С: Предприятие Конфигурация: Бухгалтерия государственного учреждения, 1С: Предприятие Конфигурация: Зарплата и кадры колледжа, Система электронного документооборота Самарской области (СЭДО),

- сведения о послевузовском профессиональном образовании;
- направление подготовки или специальность по документу об образовании;
- квалификация по документу об образовании;
- профессия;
- реквизиты трудового договора;
- характер, вид работы;
- стаж работы;
- семейное положение;
- сведения о составе семьи;
- сведения о воинском учете;
- сведения о приеме на работу и переводах на другие должности;
- сведения об увольнении;
- основание прекращения трудового договора (увольнения);
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- табельный номер;
- сведения о наградах (поощрениях);
- сведения о почетных званиях;
- сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством;
- данные об отпусках;
- сведения о владении иностранными языками;

Важно подчеркнуть, что Политика исходит из принципиального понимания невозможности достижения абсолютной защищенности информации при использовании изолированных средств защиты.

А также компоненты информационно-телекоммуникационной инфраструктуры, подлежащие защите, а именно рабочие станции, компьютеры, принтеры, МФУ, сканеры, коммутаторы, маршрутизаторы, точки доступа, vpn- координаторы HW1000, серверы, хранилища данных, защищенные каналы передачи данных. Данные информационные активы подлежат защите в соответствии с их ценностью, обязанностью Учреждения поддерживать их конфиденциальность, доступность и целостность на должном уровне. Учреждение постоянно совершенствует систему информационной безопасности в соответствии с действующим законодательством Российской Федерации и новыми возникающими угрозами информационной безопасности.

Информационная Безопасность колледжа достигается лишь путем комплексного и системного подхода, где все элементы СУИБ тесно взаимосвязаны и работают согласованно.

Это требует тщательного анализа рисков, выбора оптимальных технических и организационных мер защиты, постоянного мониторинга и адаптации системы к изменяющимся угрозам. Разработка и внедрение любых элементов информационной системы должны рассматриваться в контексте общей архитектуры безопасности, как неотъемлемая часть единой, защищенной информационной среды. При этом необходимо стремиться к оптимальному балансу между уровнем защищенности, финансовыми затратами и операционной эффективностью.

Политика предусматривает не только технические, но и организационные меры. К организационным мерам относятся разработка и утверждение внутренних нормативных актов, регламентирующих порядок доступа к информации, обработку персональных данных, использование информационных ресурсов и т.д. Обязательным элементом является обучение сотрудников вопросам информационной безопасности, повышение их осведомленности о возможных угрозах и правилах безопасного поведения. Регулярные аудиты и проверки системы безопасности позволяют оценить ее эффективность и своевременно выявлять уязвимости. Важным аспектом является взаимодействие с внешними организациями и партнерами.

Политика должна регламентировать порядок обмена информацией с внешними субъектами, обеспечивая защиту конфиденциальности и целостности данных.

Это включает в себя установление правил доступа, использование криптографических средств защиты и контроль за соблюдением договорных обязательств в сфере информационной безопасности.

Область применения настоящей Политики покрывает весь жизненный цикл (создание, эксплуатация, и ввод из эксплуатации) защищаемых информационных ресурсов колледжа. Настоящая Политика также распространяется на все деловые, финансовые, договорные, информационные, публичные и иные виды сотрудничества колледжа с третьими лицами или организациями, которые прямо или косвенно могут влиять на процессы, связанные с рисками информационной безопасности.

Таким образом, Политика информационной безопасности ГБПОУ «СМГК» – это не просто набор правил, а стратегический документ, определяющий всеобъемлющий подход к защите информационных ресурсов. Ее успешная реализация требует постоянного внимания, инвестиций в технологии и обучение персонала, а также постоянно адаптации к эволюционирующим угрозам в сфере информационной безопасности. Только системный, комплексный подход, учитывающий все аспекты – технические, организационные и человеческий фактор – позволит колледжу обеспечить необходимый уровень защищенности информации и гарантировать успешное выполнение своих уставных задач. Реализация Политики требует постоянного мониторинга, анализа и совершенствования системы защиты для обеспечения устойчивости к современным и будущим киберугрозам.

Термины и определения

1. **Авторизация** – процесс предоставления доступа к ресурсам на основе проверенной аутентификации.
2. **Аутентификация** – процесс проверки подлинности пользователя или устройства.
3. **Виртуальная частная сеть (VPN)** – технология, обеспечивающая безопасный удаленный доступ к сети через интернет.
4. **Доступность** – обеспечение доступа к информации и связанным с ней активам авторизованным пользователям в нужное время.
5. **Информационная безопасность (ИБ)** – состояние информации, при котором обеспечивается её конфиденциальность, целостность и доступность.
6. **Инцидент информационной безопасности** – событие, которое может привести к нарушению конфиденциальности, целостности или доступности информации.
7. **Конфиденциальность** – обеспечение доступа к информации только авторизованным пользователям.

8. **Межсетевой экран (брандмауэр)** – система, предназначенная для защиты сети от несанкционированного доступа.
9. **Многофакторная аутентификация (MFA)** – использование нескольких методов аутентификации для повышения безопасности.
10. **Мониторинг безопасности** – процесс наблюдения за системой или сетью для обнаружения и предотвращения угроз.
11. **Обучение и осведомленность** – программы и мероприятия, направленные на повышение знаний сотрудников в области информационной безопасности.
12. **Пароль** – секретная комбинация символов, используемая для аутентификации пользователя.
13. **План реагирования на инциденты** – набор процедур, которые описывают, как организация должна реагировать на инциденты информационной безопасности.
14. **Резервное копирование** – процесс создания копий данных для восстановления в случае их потери или повреждения.
15. **Риск** – вероятность того, что угроза воспользуется уязвимостью и приведет к ущербу.
16. **Система обнаружения вторжений (IDS)** – система, предназначенная для обнаружения попыток несанкционированного доступа или атак.
17. **Система управления информационной безопасностью (СУИБ)** – комплекс структурированных политик, процессов и технических средств, направленных на обеспечение информационной безопасности в организации.
18. **Система контроля и управления доступом (СКУД)** – комплекс оборудования, главная функция которого – ограничение доступа на охраняемый объект.
19. **Средство криптографической защиты информации (СКЗИ)** — программа или устройство, которое шифрует документы и генерирует электронную подпись.
20. **Угроза безопасности** – потенциальная возможность нарушения безопасности информации, которая может привести к ущербу.
21. **Уровень риска** – мера риска, выраженная в виде сочетания последствий и их вероятности.
22. **Учетная запись** – набор данных, который идентифицирует пользователя в системе и предоставляет доступ к ресурсам.
23. **Уязвимость** – слабое место в системе, которое может быть использовано угрозой для нарушения безопасности.
24. **Целостность** – обеспечение точности и полноты информации и методов её обработки.
25. **Шифрование** – процесс преобразования информации в форму, которая не может быть прочитана без соответствующего ключа.

Нормативные документы

Политика разработана в соответствии с законодательством Российской Федерации и требованиями Регуляторов в области информационной безопасности:

- Конституция Российской Федерации;
- Уголовный Кодекс Российской Федерации. Статья 272. Неправомерный доступ к компьютерной информации;
- Уголовный Кодекс Российской Федерации. Статья 273. Создание, использование и распространение вредоносных компьютерных программ;
- Уголовный Кодекс Российской Федерации. Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
- Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 г. № 188 (ред. от 13.07.2015 г.);
- Указ Президента РФ «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» от 01.05.2022 г. № 250 (ред. от 13.06.2024 г.);

■ Указ Президента РФ от 13.06.2024 N 500 «О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

■ Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 г. № 646;

■ Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 г. № 687 (ред. от 18.01.2025);

■ Постановление Правительства РФ ««Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. № 1119;

■ Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ (ред. 29.12.2025 г.);

■ Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ (ред. 24.06.2025 г.);

■ Федеральный закон «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ (ред. 08.08.2024 г.);

■ Федеральный закон «Об электронной подписи» от 06.04.2011 г. № 63-ФЗ (ред. 31.- 7.2025 г.);

■ Приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 г. № 21 (ред. 14.05.2020 г.);

■ Приказ ФСТЭК России «О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 г. № 21» от 14.05.2020 № 68;

■ Приказ ФСТЭК России «О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14.03.2014 г.» от 23.03.2017 № 49;

■ Приказ ФСО России «Об утверждении положения о Российском государственном сегменте информационно-телекоммуникационной сети «Интернет»» от 07.09.2016 г. № 443;

■ Приказ ФСБ России «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10.07.2014 г. № 378;

■ Приказ ФСБ России «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств» от 18.03.2025 г. № 117;

■ Методический документ. Методика оценки угроз безопасности информации, утвержденный ФСТЭК России от 05.02.2021 г.;

■ Приказ ФСТЭК России «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» от 11.04.2025 г. № 117.

■ Приказ «Об утверждении Требований к обеспечению информационной безопасности в рамках предоставления облачных услуг посредством государственной единой облачной платформы» №1106 от 2 декабря 2025 г. Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации; {СКЗИ}

■ Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утверждены руководством 8 Центра ФСБ России 31 марта 2015 года, № 149/7/2/6-432);

■ Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности (утверждены приказом ФСБ России от 10 июля 2014 года № 378).

■ Национальный стандарт РФ ИСО/МЭК 27017-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Правила применения средств обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб».

Цели, задачи и направления

Цель Политики — это внедрение, поддержка и постоянное совершенствование системы менеджмента ИБ (далее – СМИБ), которая должна обеспечивать и совершенствовать соответствующий уровень ИБ в условиях штатного функционирования и в условиях реализации угроз, защиту информации и ресурсов колледжа от внешних и внутренних угроз, связанных с умышленными и непреднамеренными действиями со стороны сотрудников и обучающихся колледжа и третьих лиц. Основная цель настоящей Политики заключается в защите информационных ресурсов от потенциального материального, физического, морального или иного ущерба, который может быть нанесен в результате случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также в минимизации рисков информационной безопасности (далее – ИБ).

Для достижения основной цели необходимо обеспечивать эффективное выполнение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ;
- создание механизма оперативного реагирования на угрозы ИБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- защита от вмешательства в процесс функционирования ИС посторонних лиц;
- соответствие требованиям Федерального законодательства, методических документов ФСБ России, ФСТЭК России, Роскомнадзор и договорным обязательствам в части ИБ;
- достижение адекватности мер по защите от угроз ИБ;
- недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников.

Область действия

Настоящая Политика распространяется на всех сотрудников и обучающихся (студентов) колледжа и обязательна для исполнения всеми его сотрудниками, обучающимися и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

Принципы политики информационной безопасности

Эти принципы учитывают комплексный подход, законодательные требования и современные вызовы в области ИБ:

Комплексность и системность. Обеспечение информационной безопасности достигается через согласованное взаимодействие технических, организационных и административных

мер. Все элементы СУИБ должны быть взаимосвязаны и интегрированы в единую архитектуру, учитывающую все аспекты защиты информации.

Конфиденциальность, целостность, доступность.

■ Конфиденциальность: доступ к информации предоставляется только авторизованным лицам или системам.

■ Целостность: гарантируется точность, полнота и неизменность информации и методов ее обработки.

■ Доступность: информация и связанные с ней ресурсы доступны авторизованным пользователям в нужное время. Риск-ориентированный подход. Защита информации основывается на регулярном анализе угроз и уязвимостей, оценке рисков и выборе мер, минимизирующих вероятность и последствия инцидентов. Меры защиты должны быть пропорциональны уровню риска.

Минимизация и оптимальность.

Меры безопасности должны обеспечивать необходимый уровень защиты при оптимальных финансовых и операционных затратах. Стремление к абсолютной безопасности не должно приводить к чрезмерным ограничениям или неоправданным расходам.

Непрерывность и адаптивность.

Система ИБ должна быть динамичной, с регулярным мониторингом, анализом и обновлением мер защиты для реагирования на новые угрозы, изменения в инфраструктуре или законодательстве. Соответствие нормативным требованиям. Политика должна соответствовать законодательству Российской Федерации.

Ответственность и обучение персонала.

Все сотрудники обязаны соблюдать правила ИБ и проходить регулярное обучение по вопросам безопасного поведения, распознавания угроз и работы с информационными системами. осведомленность персонала - ключевой фактор снижения человеческого фактора как источника уязвимостей.

Резервное копирование и восстановление.

Регулярное создание резервных копий критически важных данных и тестирование процедур восстановления для обеспечения непрерывности бизнес-процессов в случае сбоев или атак.

Прозрачность и документирование.

Все процессы, связанные с ИБ, документируются (политики, регламенты, журналы аудита). Прозрачность процессов позволяет проводить проверки, выявлять уязвимости и подтверждать соответствие требованиям.

Проактивность.

Упор делается на предотвращение инцидентов путем раннего выявления угроз, анализа тенденций в области кибербезопасности и внедрения передовых технологий защиты. Учет человеческого фактора.

Политика учитывает, что сотрудники могут быть как слабым звеном, так и важным элементом защиты. Меры включают не только обучение, но и создание корпоративной культуры, поощряющей ответственное отношение к ИБ.

Организация управления информационной безопасностью

Система управления информационной безопасностью обеспечивает координацию всех процессов ИБ в колледже. Включает политики, регламенты, технические и организационные меры, направленные на защиту информации.

Роли и ответственность:

■ Директор колледжа:

- утверждает политику ИБ и выделяет бюджет для её реализации.
- назначает ответственных за информационную безопасность.
- контролирует выполнение Политики.

■ Ответственные лица:

- разрабатывают и внедряют регламенты, процедуры и меры защиты.

-проводят обучение сотрудников, мониторинг угроз и аудит системы ИБ.

-координируют реагирование на инциденты.

■ Сотрудники и обучающиеся:

-соблюдают правила ИБ, изложенные в Политике и регламентах.

-проходят обучение и сообщают о подозрительной активности.

-несут ответственность за нарушение Политики (вплоть до дисциплинарных мер).

Регулярные совещания по обеспечению правил ИБ проводятся не реже одного раза в квартал для обсуждения угроз, инцидентов и планов улучшения.

Управление рисками информационной безопасности

Учреждение определяет и обеспечивает ресурсы, необходимые для создания, внедрения, поддержки и постоянного улучшения СОИБ Учреждения:

1) с учетом требований законодательства РФ и требований Регуляторов, определяет необходимую квалификацию для лиц, обеспечивающих СОИБ;

2) определяет, что квалификация этих лиц подтверждается соответствующим образованием, профессиональной подготовкой (стажировкой/переподготовкой) и/или опытом работы;

3) обеспечивает систематическое обучения (повышение квалификации) лиц, обеспечивающих СОИБ.

Сотрудники и лица, выполняющие работу в интересах и под контролем Учреждения, осведомляются:

- о Политике ИБ Учреждения;

- их обязанностях в обеспечение результативности СОИБ, включая пользу от их вклада в процессы улучшения СОИБ;

- последствиях несоблюдения требований СОИБ.

В Учреждении определена необходимость во взаимодействии между подразделениями, а также с третьими физическими и юридическими лицами по вопросам, имеющим отношение к СОИБ, учитывая:

- предмет взаимодействия;

- период и сроки взаимодействия;

- субъект взаимодействия;

- исполнители и роли при взаимодействии;

- процедуры осуществления взаимодействия.

Документирование информации.

СОИБ Учреждения включает:

- документационное обеспечение процессов и мер, в соответствии с законодательством РФ и требований Регуляторов в соответствующей области применения;

При создании и обновлении документации, уполномоченные сотрудники Учреждения:

- обеспечивают утверждение и сопровождение документа;

- определяют тип, формат документа и его носитель;

- проверяют и подтверждают пригодность и адекватность информации, изложенной в документах.

Осуществляется управление документационным обеспечением, необходимым для сопровождения СМИБ, с целью его соответствия принципам:

- доступности и пригодности для использования;

- надлежащей защиты от нарушения конфиденциальности, ненадлежащего использования или нарушения целостности.

Для управления документационным обеспечением в колледже осуществляется (если это применимо):

- распространение, обеспечение доступа, поиска и использования;

- хранение и обеспечение сохранности;

- управление изменениями;

- архивное хранение и уничтожение.

В соответствии с принципом риск-ориентированного подхода в колледже проводится регулярный анализ рисков информационной безопасности для выявления и минимизации угроз.

Концепция развития ИБ Учреждения отражает цели по построению и постоянному совершенствованию СМИБ. С этой целью директор колледжа утверждает иные Политики безопасности, Положения, процедуры, стандарты и нормы, обеспечивая их соблюдение.

Настоящая Политика, в том числе, определяет роль ответственного лица, отвечающего за ИБ в соответствии с требованиями законодательства РФ и внутренними нормативными документами Учреждения.

Общие принципы ИБ определяют основные необходимые действия и мероприятия, выполнение которых является обязательным условием построения защищенного рабочего процесса. Такие принципы обязательно соблюдаются всеми работниками колледжа, а также иными лицами, которые имеют доступ к информации или информационным системам колледжа. Общие положения возникают из потребностей информационной безопасности (ИБ) колледжа, определяемых путем оценки рисков в информационных системах, изучением и мониторингом законодательства РФ, требований Регуляторов и лучших международных практик по вопросам ИБ.

Общие положения устанавливают минимальный уровень безопасности, определенный в колледже, который относится ко всем сотрудникам и обучающимся колледжа и иным лицам, имеющим доступ к информации или информационным системам Учреждения. Все решения в соответствии с требованиями ИБ и безопасности информационных систем принимаются с учетом положений, описанных в настоящей Политике и тракуются как исходные требования к ИБ.

Учреждение планирует, реализует и контролирует процессы, необходимые для соответствия требованиям ИБ, а также реализует планы по достижению целей ИБ.

Учреждение выпускает и хранит документированную информацию в объеме, необходимом для обеспечения процессов СМИБ.

Учреждение управляет запланированными изменениями СМИБ и анализирует последствия внеплановых изменений, принимая меры по снижению любых неблагоприятных последствий. Процессы ИБ, осуществляемые с использованием Аутсорсинга, определяются и контролируются.

В Учреждении проводится оценка рисков ИБ через запланированные интервалы времени или в случае произошедших существенных изменений рисков ИБ.

Учреждение осуществляет обработку рисков ИБ и документирует результаты обработки рисков ИБ.

Общие положения делятся на базовые и функциональные.

Базовые положения представляют собой общие директивы, которые используются для установления и поддержания приемлемого уровня ИБ Учреждения в целом. Базовые положения являются основой определения функциональных принципов к построению и развитию СМИБ.

Функциональные принципы определяются из базовых положений. Они отражают специфические тематические области и определяют области применения СМИБ Учреждения. Совокупность защитных мер, реализующих обеспечение ИБ Учреждения, и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение, составляет Систему ИБ колледжа (далее – СИБ). Совокупность процессов менеджмента ИБ, включая ресурсное и административное (организационное) обеспечение этих процессов, составляет СМИБ колледжа. Совокупность СИБ и СМИБ составляет Систему обеспечения ИБ Учреждения (далее – СОИБ). Процессы эксплуатации защитных мер функционируют в реальном времени. Совокупность защитных мер и процессов их эксплуатации должна обеспечивать текущий требуемый уровень ИБ в условиях штатного функционирования, а также в условиях реализации угроз, учтенных в моделях Учреждения и приводящих к возникновению локальных Инцидентов ИБ. СОИБ определена, спланирована,

регламентирована внутренними нормативными документами Учреждения, постоянно контролируется и совершенствуется, во избежание деградации системы защиты и возрастанию рисков ИБ. Для поддержания системы защиты на должном уровне, в качестве оперативной меры, используется мониторинг событий и Инцидентов в СИБ. Для оценки состояния ИБ защищаемого актива и выявления признаков деградации используемых защитных мер проводится оценка (самооценка) соответствия системы актуальным нормам законодательства РФ и требованиям Регуляторов в области ИБ. Указанные процессы составляют СМИБ Учреждения.

Процесс управления рисками:

Анализ угроз и уязвимостей: Проводится не реже одного раза в год с использованием методик ФСТЭК России.

Угрозы включают кибератаки, утечки данных, сбои оборудования.

Уязвимости выявляются через сканирование систем и аудит.

Оценка рисков: Риски оцениваются по вероятности и потенциальному ущербу (низкий, средний, высокий). Например, утечка персональных данных классифицируется как высокий риск.

При планировании СМИБ Учреждение учитывает внутренние и внешние факторы своей деятельности и требования, сторон, имеющие отношение к СМИБ, а также определяет подлежащие рассмотрению риски ИБ и возможности Учреждения с целью:

1. обеспечения способности достижения намеченных результатов СМИБ;
2. предотвращения или митигации нежелательных последствий (например, реализации рисков ИБ);
3. обеспечения постоянного улучшения (например, уровня ИБ);
4. планирования действий по рассмотрению данных рисков и возможностей;
5. оценки результативности процессов СМИБ.

Колледж (Учреждение) определяет и внедряет процесс оценки рисков ИБ, который позволяет:

1. устанавливать и поддерживать критерии рисков ИБ, включая: критерии принятия рисков ИБ и критерии для проведения оценки рисков ИБ;
2. обеспечивать достоверные и сопоставимые результаты повторных оценок рисков ИБ;
3. применять процесс оценки рисков ИБ для идентификации рисков, связанных с нарушением Конфиденциальности, Целостности и Доступности информации в рамках СМИБ и идентифицировать владельцев рисков ИБ;
4. проводить анализ рисков ИБ:

- оценивать потенциальные последствия, которые могут произойти в результате реализации рисков ИБ;

- оценивать реальную Вероятность реализации рисков ИБ;

- определять уровни рисков ИБ;

5. оценивать риски ИБ:

- сравнивать результаты анализа рисков ИБ;

- определять приоритетность обработки проанализированных рисков ИБ.

Учреждение определяет и применяет процесс обработки рисков ИБ с целью:

- выбора подходящих вариантов обработки рисков ИБ, учитывая результаты оценки рисков ИБ;

- определения всех мер и средств ИБ, необходимых для реализации выбранного(ых) варианта(ов) обработки рисков ИБ.

- сравнения мер и средств ИБ;

- подготовки ведомости применимости мер и средств ИБ, которая содержит:

- 1) необходимые меры обеспечения информационной безопасности и обоснования их применения;

- 2) информацию о том, реализованы или нет необходимые меры обеспечения ИБ;

- 3) обоснования неприменения мер и средств ИБ;

4) разработки плана обработки рисков ИБ;

5) согласования и (или) утверждения плана обработки рисков ИБ и принятия остаточных рисков ИБ владельцами рисков. Учреждение документирует информацию о процессе оценки рисков ИБ.

План управления рисками.

Для каждого риска разрабатываются меры:

■ Технические: внедрение межсетевых экранов, шифрования, антивирусов.

■ Организационные: обучение сотрудников, регламенты доступа. Мониторинг и пересмотр. План рисков обновляется при внедрении новых систем, изменении законодательства или появлении новых угроз.

Ответственным за управление рисками является специалист по защите информации, назначенный приказом директор колледжа.

Все сотрудники обязаны сообщать о выявленных уязвимостях или подозрительной активности.

Технические меры защиты в колледже используются современные технологии для защиты информации в соответствии с принципом многоуровневой защиты.

Ключевые меры:

■ Межсетевые экраны (брандмауэры): Фильтруют сетевой трафик, предотвращая несанкционированный доступ. Настраиваются для блокировки подозрительных IP-адресов.

■ Шифрование: Все конфиденциальные данные защищаются сертифицированными СКЗИ при хранении и передаче. Используются протоколы TLS для сетевых соединений, защищенные каналы связи для передачи информации.

■ Многофакторная аутентификация (MFA): Применяется для доступа к ключевым устройствам.

■ Резервное копирование: Критические данные резервируются ежемесячно, копии хранятся в защищенном месте.

■ Антивирусное ПО: Ключевые устройства оснащены антивирусами с автоматическим обновлением. Проводятся автоматические проверки на вредоносное ПО.

■ Обновление ПО: Системы и приложения обновляются для устранения уязвимостей автоматически или при необходимости. Организационные меры защиты Организационные меры обеспечивают соблюдение правил ИБ всеми сотрудниками в соответствии с принципами контроля доступа и прозрачности. Ключевые меры.

■ Контроль доступа.

Пароли должны быть сложными (не менее 8 символов, включая буквы, цифры, символы) и обновляться каждые полгода.

■ Политика чистого стола и чистого экрана.

Конфиденциальные документы хранятся в запираемых шкафах. Рабочие станции блокируются автоматически через 5 минут бездействия.

■ Правила использования ресурсов.

Электронная почта используется только для рабочих задач, с фильтрацией входящих сообщений. Доступ в интернет осуществляется с фильтрацией контента. Личные устройства допускаются к корпоративной сети только после проверки заведующим центром программного информационного технологического сопровождения образовательного процесса колледжа.

■ Обработка конфиденциальной информации.

Конфиденциальные данные обрабатываются в защищенных системах с использованием шифрования.

■ Утилизация носителей.

Носители информации (бумажные, электронные) уничтожаются сертифицированными методами (например, шредирование, перезапись данных). Все сотрудники обязаны ознакомиться с организационными мерами. Нарушение правил влечёт дисциплинарную ответственность.

Безопасность сотрудников и обучающихся.

Сотрудники и обучающиеся являются ключевым элементом системы информационной безопасности, и их действия регулируются для снижения рисков, связанных с человеческим фактором, в соответствии с принципом ответственности и обучения.

Ключевые меры.

■ Соглашения о конфиденциальности. Все сотрудники подписывают соглашение о неразглашении персональных данных. Соглашение включает ответственность за нарушение правил ИБ.

■ Обучение ИБ. При трудоустройстве проводится вводный инструктаж по ИБ (правила паролей, распознавание фишинга, работа с данными). Обучение документируется, а участие является обязательным.

■ Процедуры при увольнении или переводе.

Доступ к системам блокируется в течение 24 часов после увольнения.

■ Проводится аудит активности сотрудника за последний месяц. Сотрудник возвращает все носители информации и оборудование. Руководство обеспечивает финансирование программ обучения, а ответственные лица координируют их проведение. Нарушение правил ИБ сотрудниками влечёт дисциплинарные меры.

Требования по информационной защите

Требования по информационной защите формируются для следующих областей:

- 1) управление доступом;
- 2) категорирование и обработка информации;
- 3) физическая безопасность и защита от воздействий окружающей среды;
- 4) области, ориентированные на конечного пользователя (информационные активы, передача информации, дистанционная работа, ограничения в работе);
- 5) резервное копирование;
- 6) защита от вредоносного кода (антивирусная защита);
- 7) управление техническими уязвимостями;
- 8) криптография;
- 9) безопасность коммуникаций;
- 10) конфиденциальность и защита персональных данных.

Владельцы активов, совместно с ответственным за ИБ сотрудником, определяют соответствующие правила управления доступом, права доступа и ограничения для конкретных ролей сотрудников Учреждения по отношению к своим активам с уровнем детализации и набором мер, отражающих риски, связанные с обеспечением ИБ. Как логические, так и физические меры по управлению доступом рассматриваются совместно. В колледже учитываются:

- требования к безопасности прикладного программного обеспечения, в том числе работающему по сети Интернет;
- политика обработки персональных данных;
- механизмы авторизации учетных записей пользователей, соответствие между правами доступа и должностными обязанностями сотрудников;
- разделение ролей по управлению доступом, администрирование доступа;
- требования к периодическому пересмотру прав доступа;
- логирование записей всех значимых событий, касающихся использования и управления идентификаторами пользователей и закрытой аутентификационной информацией.

В отношении использования сетей и сетевых сервисов учитываются:

- сети и сетевые сервисы, к которым разрешен доступ;
- процедуры авторизации для определения ролей и разрешений доступа к сетям и сетевым сервисам;
- средства, используемые для доступа к сетям и сетевым сервисам VPN или беспроводным сетям;

- требования к аутентификации и авторизации пользователя для доступа к различным сетевым сервисам;
- мониторинг использования технических средств, программного обеспечения, сетевых сервисов и ресурсов.

Процесс управления идентификаторами сотрудников колледжа включает:

- использование уникальных идентификаторов пользователей, позволяющих фиксировать несанкционированные действия пользователей;
- своевременное отключение или удаление идентификаторов уволенных сотрудников;
- выявление и удаление/блокирование избыточных идентификаторов пользователей;
- исключение возможности передачи идентификаторов пользователей другим пользователям и третьим лицам;
- безопасное хранение учетных записей пользователей;
- требования к парольной защите.

Процесс предоставления или аннулирования прав доступа и регламентированных действий для идентификаторов пользователей включает:

- проверку предоставления уровня доступа соответствующего политикам доступа;
- недопущение активации права доступа (в том числе поставщикам/поставщиками услуг) до завершения процедур аутентификации;
- корректировку прав доступа пользователей, у которых поменялись роли или задачи;
- периодический контроль, а при необходимости, пересмотр права доступа совместно с владельцами информационных систем или сервисов.

При пересмотре прав доступа учитываются:

- пересмотр прав доступа, как через определенные интервалы времени, так и после любых изменений статуса работников (таких как изменение в должности, или увольнение);
- регулярные проверки назначенных привилегий. Сотрудники осведомлены:
- о необходимости тайного хранения парольной и ключевой информации, исключая ее компрометацию;
- о недопустимости открытого хранения парольной и ключевой информации (например, на бумаге, в файле программного обеспечения или на мобильном устройстве), кроме тех случаев, когда эти записи могут быть надежно сокрыты;
- о необходимости изменять парольную информацию всякий раз, когда есть какие-либо подозрения или признаки ее возможной компрометации;
- о необходимости использования уникальных, сложных паролей с регламентированной минимальной длиной 8 символов;
- о недопустимости использования корпоративных ресурсов в личных целях; В отношении всех информационных активов колледжа, активов, находящихся под контролем колледжа, а также активов, используемых для доступа к инфраструктуре колледжа, должна быть определена ответственность соответствующего сотрудника.

Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами колледжа доводится до сведения директора колледжа. Внос в здание и помещения колледжа личных портативных компьютеров и внешних носителей информации (диски, флеш-карты и т.п.), а также вынос их за пределы колледжа производится только при согласовании с заведующим центром программного информационного технологического сопровождения образовательного процесса колледжа. Все данные, составляющие тайну ГБПОУ «СМГК» и хранящиеся на внешних жестких дисках, портативных компьютерах, должны быть зашифрованы. Все работы в пределах колледжа должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию администрацией. В целях обеспечения санкционированного доступа к информационным ресурсам колледжа любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля. Пользователи обязаны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования.

Запрещается сообщать свой пароль другим лицам или предоставлять доступ к служебному компьютеру третьим лицам. В процессе работы сотрудники обязаны использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не более 15 минут.

Каждый сотрудник обязан немедленно уведомить заведующего центром программного информационного технологического сопровождения образовательного процесса колледжа обо всех случаях предоставления доступа третьим лицам к ресурсам сети колледжа. Доступ к сети Интернет обеспечивается только в служебных целях и не может использоваться для незаконной деятельности. Запрещается посещение сайтов, содержащих оскорбительный, противозаконный или неэтичный контент.

Сотрудники обязаны обеспечивать физическую безопасность оборудования, на котором хранится информация колледжа, включая компьютеры, ноутбуки и периферийные устройства.

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит центр программного информационного технологического сопровождения образовательного процесса колледжа. Все ключевые рабочие станции должны быть оснащены антивирусным программным обеспечением.

Сотрудникам запрещается блокировать, изменять настройки или устанавливать иное антивирусное ПО. Сотрудники обязаны регулярно создавать резервные копии всех основных служебных данных и программного обеспечения, используемых в рабочих процессах.

Физическая безопасность

Физическая безопасность предотвращает несанкционированный доступ, кражу или повреждение информационных активов в соответствии с принципом многоуровневой защиты.

В колледже определены границы контролируемой зоны кабинетов, где производится непосредственная обработка конфиденциальной информации, а также организован и осуществляется пропускной и внутриобъектовый режим. Функционирует периметровое видеонаблюдение. Доступ в помещения колледжа предоставлен только авторизованному персоналу.

Ключевые меры.

■ Видеонаблюдение и сигнализация. Критические зоны находятся под круглосуточным видеонаблюдением. Установлены пожарные и охранные сигнализации с уведомлением службы безопасности.

■ Контроль доступа посетителей.

Все посетители регистрируются на входе и сопровождаются сотрудниками.

■ Сторонние службы.

Техническое обслуживание и другие службы работают под надзором.

■ Защита от физических угроз. Ключевые рабочие станции защищены от перебоев питания с помощью системы резервного питания. Заведующий центром программного информационного технологического сопровождения образовательного процесса колледжа обеспечивает техническое обслуживание оборудования.

Управление инцидентами информационной безопасности

В соответствии с принципом реагирования на инциденты в колледже разработаны процедуры для обнаружения, локализации и устранения инцидентов ИБ, таких как утечки данных, кибератаки или сбои.

Процесс управления инцидентами.

Сотрудники колледжа, использующие или имеющие доступ к информационным активам Учреждения, осведомлены о требованиях ИБ, относящихся к конфиденциальной информации, обрабатываемой на рабочих станциях. В Учреждении действует правило

«чистого стола» в отношении бумажных документов и сменных носителей информации, а также политика «чистого экрана» для средств обработки информации. Политика «чистого стола» и «чистого экрана» учитывает категории информации, законодательные и внутренние нормативные требования, а также соответствующие риски, связанные с информационной безопасностью Учреждения. Меры обеспечения ИБ, которым необходимо следовать при использовании средств связи для передачи информации, учитывают:

- использование криптографических методов, в том числе для защиты Конфиденциальности, Целостности,

Доступности и аутентичности информации;

- внутренние нормативные документы, определяющие сроки хранения и утилизации информации, учитывающие нормы и требования законодательства РФ;

- использование антивирусной защиты при работе в программно

- прикладном обеспечении, в котором происходит обработка персональных данных, в том числе для защиты информации ограниченного доступа в электронном виде, передаваемой в форме вложения;

При удаленной работе сотрудники колледжа должны обеспечить отсутствие несанкционированного просмотра экрана рабочего монитора третьими лицами. При удаленном доступе пользователей к информационным системам и содержащейся в них информации принимаются меры по защите информационных систем и содержащейся в них информации и, при необходимости, обеспечивается защита каналов передачи данных, используемых для осуществления удаленного доступа.

■ Определение инцидента событие, нарушающее целостность, конфиденциальность, или доступность информации, например, фишинговая атака, сбой сервера).

■ Обнаружение.

Сотрудники обязаны сообщать о подозрительной активности в течение 1 часа.

■ Локализация.

Блокировка заражённых учётных записей или устройств. Отключение поражённых систем от сети.

■ Устранение.

Восстановление данных из резервных копий. Устранение уязвимостей (например, обновление ПО).

■ Анализ.

Выявление причин инцидента и оценка ущерба. Разработка мер для предотвращения повторения.

■ Уведомление.

Резервные копии информации и программного обеспечения создаются на регулярной основе. Предусмотрены надлежащие средства резервного копирования, обеспечивающие возможность восстановления всей важной информации и ПО после аварии, сбоя носителя или иного Инцидента.

При выполнении резервного копирования учитываются следующие меры:

- ведется точный и полный учет резервных копий, а также документирование процедур восстановления;

- объем (например, полное или частичное резервное копирование) и частота резервного копирования соответствуют требованиям безопасности, а также важности информации для непрерывной работы;

- резервированная информация имеет соответствующий уровень защиты, как физической, так и от угроз окружающей среды;

- резервные копии, содержащие информацию конфиденциального характера, защищаются с помощью шифрования.

Эксплуатационные процедуры контролируют выполнение резервного копирования и обрабатывают результаты в ходе запланированного резервного копирования, чтобы обеспечить полноту и результативность резервного копирования в соответствии с политикой

резервного копирования. Периодичность резервного копирования, количество, типы носителей, места хранения резервных копий и уровень критичности резервируемой информации определяются во внутренних регламентах колледжа по защите информации.

Информация, необходимая для поддержки управления уязвимостями прикладного программного обеспечения, включает в себя информацию о разработчике ПО, номерах версий, текущем состоянии развертывания (например, какое ПО установлено в каких системах), а также доступе к системе, ее конфигурациям и компонентам ПО. Информация об уязвимостях прикладного программного обеспечения, используемого для обработки персональных данных берется из базы данных угроз ФСТЭК bdu.fstec.ru. Порядок выявления, оценки и устранения уязвимостей прикладного программного обеспечения определены во внутреннем нормативном документе.

При работе с СКЗИ учитывается следующее:

- использование шифрования для защиты информации, передаваемой с помощью носителей, а также иных каналов связи;
- меры к управлению ключами, в том числе методы по защите криптографических ключей и восстановлению зашифрованной информации в случае утери, компрометации или повреждения ключей;
- роли и обязанности ответственных за направление СКЗИ;
- законодательство, требование Регуляторов, стандарты, регулирующие деятельность, связанную с использованием СКЗИ; Регламентация процессов, связанных с криптографической защитой в Учреждении учитывает следующие ключевые меры:
- обеспечение конфиденциальности при использовании шифрования для защиты информации ограниченного доступа как при хранении, так и при передаче;
- обеспечение целостности и аутентичности при использовании электронных подписей, для проверки подлинности или целостности информации ограниченного доступа, при ее передаче и хранении;
- обеспечение неотказуемости при использовании криптографических методов, с целью подтверждения наличия (или отсутствия) события или действия;
- использование криптографических методов для аутентификации и авторизации пользователей при обработке персональных данных в прикладном программном обеспечении;

В колледже уделяется особое внимание защите персональных данных и считается подобную информацию одним из важнейших активов. Конфиденциальность и защита персональных данных обеспечивается в строгом соответствии с требованиями соответствующих законодательных и нормативных актов РФ и требований Регуляторов. Процедуры, регламентирующие порядок работы с персональными данными в колледже определены и задокументированы. За обработку и обеспечение безопасности персональных данных назначены ответственные работники, исходя из принципа минимально необходимого круга лиц.

Приняты подходящие технические и организационные меры для защиты персональных данных. Порядок работы с персональными данными и их защиты в колледже регулируются Политикой в отношении обработки персональных данных. Политика подлежит пересмотру в случае изменений в законодательные и нормативные документы Российской Федерации и требований Регуляторов.

При утечке персональных данных регуляторы уведомляются в течение 72 часов в соответствии с ФЗ-152. Все инциденты регистрируются в журнале, который ведёт ответственное лицо. Ежегодно проводятся учения для подготовки к инцидентам. Отчёт об инцидентах предоставляется директору колледжа в течение 5 дней после устранения. Взаимодействие с внешними сторонами В соответствии с принципом защиты при взаимодействии с внешними сторонами колледж обеспечивает безопасность обмена данными с партнёрами, подрядчиками и другими субъектами.

Ключевые меры

■ Защищённые каналы связи.

Обмен данными осуществляется через защищённые системы ЭДО, использующие протоколы с шифрованием (TLS). Используются сертифицированные СКЗИ для защиты конфиденциальных данных.

■ Договорные обязательства.

Договоры с внешними сторонами включают пункты о соблюдении стандартов ИБ. Указывается ответственность за утечки данных или нарушения.

Реализация политики информационной безопасности

Реализация Политики информационной безопасности ГБПОУ «СМГК» осуществляется на основе нормативных документов, определяющих порядок выполнения процедур и процессов, связанных с профессиональной деятельностью в колледже. Порядок внесения изменений и дополнений в политику информационной безопасности Изменения и дополнения в Политику информационной безопасности вносятся не реже одного раза в три года для обеспечения соответствия установленных мер защиты актуальным условиям и требованиям законодательства в области информационной безопасности.

Контроль за соблюдением политики информационной безопасности

Текущий контроль за соблюдением требований Политики информационной колледжа возлагается на специалиста по защите информации, назначенного приказом директора колледжа. Заведующий центром программного информационного технологического сопровождения образовательного процесса колледжа регулярно анализирует выполнение и соблюдение положений Политики информационной безопасности, а также осуществляет последующий контроль за исполнением ее требований.

Ответственность за нарушение Политики безопасности

Сотрудники осведомлены об административной ответственности за нарушение требований по защите информации и установленных Учреждением правил обработки информации, и любое нарушение правил находится в зоне их ответственности, а именно: В случае нарушения порядка получения и обработки персональных данных, а также их распространение, предусмотрена административная ответственность по ст. 13.11 КоАП РФ. Данной статьей предусмотрено наказание в виде наложения административного штрафа на должностных лиц – от десяти тысяч до восьмисот тысяч рублей. Пациенты, чьи данные были раскрыты третьим лицам без их согласия, вправе обратиться в суд для взыскания денежной компенсации. Ответственность за выполнение правил политики безопасности несет каждый сотрудник колледжа в рамках своих служебных обязанностей и полномочий. На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования Политики, 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 колледжу в результате нарушения ими правил Политики (Ст. 238 Трудового кодекса Российской Федерации).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники колледжа несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

Лист ознакомления:

Баринова Ю.Ю.
Бакланов В.Г.
Бутузова Н.Н.
Антонова Н.А.
Биркалова Т.Н.
Брыкалова Т.В.
Жук М.В.
Жук Е.Г.
Зырянова Ю.А.
Кажаева Н.С.
Калямина А.В.
Капустина Т.В.
Киричевская Т.А.
Королева Л.А.
Кружилин П.В.
Кузнецова О.К.
Куликова Н.А.
Шилина Т.И.
Клюйкова И.С.
Студеникин Ю.Е.
Артюшина А.А.
Клюйкова И.С.
Молебнова Н.В.
Щадрин М.Л.

Лаптева Е.С.
Марыскина О.П.
Минеева Ю.Ю.
Амиров И.Р.
Мухамедова В.Г.
Никитина Е.М.
Новоженкина С.А.
Плаксина Е.П.
Полушкина О.А.
Потапов А.Ф.
Прищепа В.В.
Родина Е.И.
Слонова О.А.
Токарев Д.В.
Филиппова В.Ф.
Фридрих Л.В.
Худышева О.Г.
Рябов А.Ю.
Кузьмина Г.И.
Биркалова Т.Н.
Бессараб Т.В.
Курдова О.А.
Тораманова С.И.
Щепалова С.Ю.