

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

ИКБ направление «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Практическая работа № 1

**Политика информационной безопасности**

**ФГБУ «Редакция «Российской газеты»**

по дисциплине

«Управление информационной безопасностью»

Группа:

ББМО-02-22

Выполнил:

Агишевский П. Д.

Проверил:

Пимонов Р. В.

Москва, 2024

**СОДЕРЖАНИЕ**

[1. Обозначения и сокращения 3](#_Toc162382965)

[2. Термины и определения 3](#_Toc162382966)

[3. Область применения 3](#_Toc162382967)

[4. Нормативные ссылки 5](#_Toc162382968)

[5. Общие положения 5](#_Toc162382969)

[6. Положения по информационной безопасности 6](#_Toc162382970)

[7. Задачи системы управления ИБ 7](#_Toc162382971)

[8. Реализация 8](#_Toc162382972)

[8.1. Структура и ответственность 9](#_Toc162382973)

[8.2. Осведомленность и информирование 9](#_Toc162382974)

[8.3. Реагирование на инциденты безопасности 9](#_Toc162382975)

[9. Контроль 10](#_Toc162382976)

[10. Совершенствование 10](#_Toc162382977)

[Приложение 1 11](#_Toc162382978)

[Приложение 2 17](#_Toc162382978)

# **1.** **Обозначения и сокращения**

В настоящем документе использованы следующие сокращения:

|  |  |
| --- | --- |
| **ИБ** | * Информационная безопасность |
| **ИС** | * Информационная система |
| **СУИБ** | * Система управления информационной безопасностью |

# **2.** **Термины и определения**

Термины и определения, используемые в настоящей Политике и рекомендуемые к использованию в нормативных и организационно- распорядительных документах, созданных на ее основе, приведены в Приложении № 1 «Термины и определения».

# **3.** **Область применения**

3.1. Настоящая Политика информационной безопасности (далее – «Политика») предназначена для обеспечения информационной безопасности в ФГБУ «Редакция «Российской газеты» (далее «Организация»), а также для установления обязательных норм и требований к системе управления информационной безопасностью.

3.2. Система обеспечения ИБ представляет собой совокупность защитных мер, включающий в себя юридические, организационные и технические инструменты, необходимые для обеспечения непрерывной безопасности конфиденциальных данных в Организации.

3.3. Система управления ИБ является составной частью общей системы управления Организации, обеспечивает поддержку и управление процессами обеспечения ИБ на всех этапах деятельности корпоративной информационной системы.

3.4. Организация разрабатывает и внедряет систему управления ИБ, отвечающую требованиям и рекомендациям нормативных документов Российской Федерации.

3.5. Основные цели внедрения системы управления ИБ Организации:

* минимизация утраты или кражи конфиденциальных данных;
* своевременное выявление, оценка и прогнозирование потенциальных источников угроз для информационной безопасности;
* обеспечение бесперебойного функционирования бизнес-процессов;
* гарантирование целостности данных, включая защиту от несанкционированных изменений;
* обеспечение непрерывного доступа к необходимым данным путем предотвращения атак, таких как DDoS, направленных на снижение доступности системы.

3.6. Положения настоящей Политики распространяются на все виды информации в Организации, хранящейся либо передающейся любыми способами, в том числе информацию, зафиксированную на материальных носителях.

3.7. Положения настоящей Политики также распространяются на средства приема, обработки, передачи, хранения и защиты информации Организации.

3.8. Политика применяется ко всем сотрудникам и сторонним лицам, имеющим доступ к информационным ресурсам Организации.

3.9. Область применения настоящей Политики распространяется на все подразделения Организации, в которых обрабатывается информация, не составляющая государственную тайну.

# **4.** **Нормативные ссылки**

При разработке настоящей Политики учтены требования и рекомендации следующих документов:

* ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
* ГОСТ Р ИСО/МЭК 27002-2021 «Информационная технология (ИТ);
* Федеральный закон от 29.07.2004 г. №98-ФЗ «О коммерческой тайне».
* Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

# **5.** **Общие положения**

Для обеспечения информационной безопасности необходимо принимать следующие меры:

5.1. Установление и поддержка политики информационной безопасности.

5.2. Обучение и осведомленность сотрудников: все сотрудники должны быть обучены основам информационной безопасности и должны быть в курсе текущих угроз и средств защиты.

5.3. Управление доступом: установление и контроль доступа к информации с помощью паролей, аутентификации и разграничения прав доступа.

5.4. Контроль сетевой безопасности: установление мер для защиты сетей и систем от несанкционированного доступа, включая использование брандмауэров, антивирусного программного обеспечения и системы обнаружения вторжений.

5.5. Защита данных: использование шифрования и других методов защиты данных на всех этапах их передачи и хранения.

5.6. Аудит безопасности: регулярное проведение аудитов информационной безопасности для выявления уязвимостей и неправильного использования систем.

5.7. Физическая безопасность: защита серверных комнат, центров обработки данных и других физических объектов, содержащих информацию, от несанкционированного доступа.

5.8. Регулярное обновление и обслуживание программного обеспечения: установка последних обновлений и патчей для операционных систем и приложений с целью закрытия уязвимостей.

5.9. Резервное копирование и восстановление данных: создание резервных копий данных и регулярное тестирование процедур восстановления для минимизации потерь в случае сбоя или взлома.

5.10. Управление рисками: идентификация и оценка рисков, связанных с информационной безопасностью, и принятие соответствующих мер для их снижения или устранения.

Соблюдение политики информационной безопасности и всех принятых мер является обязанностью каждого сотрудника и помогает обеспечить защиту информации.

# **6.** **Положения по информационной безопасности**

6.1. Положения по информационной безопасности Организации (далее – «Положения») разрабатываются на основании Политики информационной безопасности Организации в целях создания, развития и совершенствования общей системы защиты информации Организации.

6.2. Положения по ИБ являются приложениями к настоящей Политике.

- Правила о защите вредоносного программного обеспечения определены в «Положении о защите вредоносного программного обеспечения» (Приложение №2).

6.3. Принятие новых Положений, а также пересмотр или отмена действующих Положений оформляется документально и утверждается приказом директора Организации.

6.4. Актуализация Положений осуществляется при изменении законодательной или нормативной базы в области ИБ, а также при изменении внутренней ситуации в Организации.

# **7.** **Задачи системы управления ИБ**

7.1. Основной целью управления ИБ является обеспечение защиты, конфиденциальности, целостности и доступности информации и информационных ресурсов Организации.

7.2. Основными задачами управления ИБ являются:

Обучение и информирование сотрудников по вопросам информационной безопасности и контроль их соблюдения установленных правил и процедур;

* Установление и контроль доступа к информации с помощью паролей, аутентификации и разграничения прав доступа;
* Установление мер для защиты сетей и систем от несанкционированного доступа, включая использование брандмауэров, антивирусного программного обеспечения и системы обнаружения вторжений;
* Регулярное проведение аудитов информационной безопасности для выявления уязвимостей и неправильного использования систем;
* Защита серверных комнат, центров обработки данных и других физических объектов, содержащих информацию, от несанкционированного доступа;
* Установка последних обновлений и патчей для операционных систем и приложений с целью закрытия уязвимостей;
* Определение и классификация информации с учетом ее важности и уровня конфиденциальности.
* Разработка и применение защитных мер для сохранения информации, включая технические, организационные и процедурные.
* Мониторинг и анализ инцидентов информационной безопасности, а также проведение расследований в случае несанкционированных инцидентов.
* Регулярная оценка рисков, связанных с информационной безопасностью, и внесение изменений в меры по их снижению.
* Создание резервных копий данных и регулярное тестирование процедур восстановления для минимизации потерь в случае сбоя или взлома;
* Идентификация и оценка рисков, связанных с информационной безопасностью, и принятие соответствующих мер для их снижения или устранения.

7.3. В основе управления ИБ Организации лежит подход, отраженный в модели деятельности в виде циклического процесса «планирование – реализация – контроль – совершенствование» (по ГОСТ Р ИСО/МЭК 27001-2021).

7.4. Организация осуществляет деятельность по управлению рисками, повышению осведомленности сотрудников и реагированию на инциденты в области ИБ. Регулярно, не реже одного раза в два года, производится анализ состояния рисков, связанных с ИБ. Защитные меры должны основываться на всесторонней оценке этих рисков и должны быть им соразмерны.

7.5. Всю ответственность за защиту своей информации и информационных ресурсов Организация возлагает на руководителей структурных подразделений. Руководители структурных подразделений Организации обязаны соблюдать требования Политики информационной безопасности и Положений, а также обеспечивать их выполнение со стороны всех сотрудников Организации.

# **8.** **Реализация**

Реализация системы управления ИБ осуществляется на основе четкого распределения ролей и ответственности в области информационной безопасности.

# **8.1.** **Структура и ответственность**

8.1.1. Ответственное лицо, назначенное приказом директора Организации, руководит работами по внедрению и совершенствованию СУИБ, в том числе организует выполнение Положений по ИБ.

8.1.2. Ответственными лицами являются руководители подразделений. Их задачи включают в себя обеспечение выполнения требований Политики и Положений по ИБ.

8.1.3. Функции администраторов по ИБ возлагаются на руководителей направлений по каждому структурному подразделению.

8.1.4. Ответственность работников Организации за надлежащее выполнение требований и правил ИБ определена в положениях, правилах, регламентах и другие внутренних нормативных и организационно распорядительных документах Организации.

# **8.2.** **Осведомленность и информирование**

Доведение правил ИБ до сотрудников Организации проводится: при приеме на работу; во время регулярных обучений сотрудников; в ходе производственных совещаний; профессиональной подготовки персонала; тренингов по ИБ.

# **8.3.** **Реагирование на инциденты безопасности**

8.3.1. Для определения возможных сценариев восстановления информационной системы Организации в чрезвычайных ситуациях, конкретизации технических средств и действий работников и структурных подразделений по локализации инцидентов ИБ должны быть разработаны планы восстановительных работ для важных информационных ресурсов.

# **9.** **Контроль**

Объектами контроля ИБ являются: конфиденциальная информация, информационные ресурсы компании, оборудование и средства защиты информации.

Контроль над соблюдением Политики и ее актуальности производится лицом, назначенным директором Организации.

# **10.** **Совершенствование**

Порядок совершенствования системы управления информационной безопасностью Организации:

– Мониторинг информационной безопасности должно осуществляться для всех систем Организации, чтобы выявлять аномалии в их функционировании.

– Анализ результатов аудитов и проверок системы управления информационной безопасностью.

– При улучшении существующих систем необходимо учесть потребность в обеспечении безопасности.

– Следует разработать рекомендации для улучшения системы управления информационной безопасностью путем внедрения новых мер и повышения эффективности имеющихся защитных мер Организации.

– Внутренние положения Организации должны быть разработаны строго в соответствии с Информационной безопасностью Организации.

– Все внутренние положения Организации могут быть приняты, пересмотрены или отменены.

Приложение № 1

к Политике информационной безопасности

ФГБУ «Редакция «Российской газеты»

# **Термины и определения**

**Автоматизированная система** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (ГОСТ 34.003-90).

**Аудит информационной безопасности** - систематический, независимый и документируемый процесс получения свидетельств деятельности по обеспечению информационной безопасности и установлению степени выполнения критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации (ГОСТ Р 53114-2008).

**Аутентификация** - действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации (ГОСТ Р 58833-2020).

**Безопасность информации (данных)** - состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность (ГОСТ Р 53114-2008).

**Безопасность информационной технологии** - состояние защищенности информационной технологии, при котором обеспечиваются безопасность информации, для обработки которой она применяется, и информационная безопасность информационной системы, в которой она реализована (ГОСТ Р 53114-2008).

**Блокирование информации (данных)** - временное прекращение сбора, систематизации, накопления, использования, распространения информации, в том числе ее передачи.

**Вредоносная программа** - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационных систем (ГОСТ Р 51275-2006).

**Доступ к информации (данным)** - ознакомление с информацией, её обработка, в частности, копирование модификация или уничтожение информации. Доступ к информации - возможность получения информации и её использования.

**Защищаемая информация (защищаемые данные)** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов (ГОСТ Р 53114-2008).

**Идентификация риска** - процесс обнаружения, распознавания и описания рисков (ГОСТ Р 53114-2008).

**Информационная безопасность** - состояние защищенности интересов организации в условиях угроз в информационной сфере. (ГОСТ Р 53114- 2008).

**Информационная инфраструктура** - совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам (по ГОСТ Р 53114-2008).

**Информационные ресурсы** - совокупность данных и/или документов, представленных в любой знаковой системе, на любом физическом носителе и/или распространяемых в информационно-телекоммуникационных сетях и организованных для эффективного получения достоверной информации.

**Информационная система** - система, представляющая собой совокупность информации, а также информационных технологий и технических средств, позволяющих осуществлять обработку информации с использованием средств автоматизации или без использования таких средств.

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

**Инцидент информационной безопасности** - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность (по ГОСТ Р 53114-2008).

**Источник угрозы безопасности** - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Конфиденциальная информация** - документированная информация, доступ к которой ограничивается в соответствии с законодательством.

**Управление ИБ** - скоординированные действия по руководству и управлению в части обеспечения информационной безопасности в соответствии с изменяющимися условиями внутренней и внешней среды (по ГОСТ Р 53114-2008).

**Управление рисками ИБ** - скоординированные действия по руководству и управлению в отношении рисков ИБ с целью их минимизации (по ГОСТ Р 53114-2008).

**Меры обеспечения ИБ** - совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности.

**Мониторинг ИБ** - Непрерывное наблюдение за состоянием и поведением объектов ИБ с целью их контроля, оценки и прогноза в рамках управления ИБ.

**Нарушитель ИБ** - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах.

**Несанкционированный доступ (несанкционированные действия)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

**Носитель информации (данных)** - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Обеспечение ИБ** - деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности или на минимизацию ущерба от возможной реализации таких угроз (ГОСТ Р 53114-2008).

**Обработка информации (данных)** - действия (операции) с информацией, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение информации.

**Объект защиты информации** - информация либо носитель информации, или информационный процесс, которую (который) необходимо защищать в соответствии с целью защиты информации (ГОСТ Р 53114-2008).

**Объект информатизации** - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены (ГОСТ Р 53114-2008).

**Оценка риска** - процесс, объединяющий идентификацию риска, анализ риска и их количественную оценку (ГОСТ Р 53114-2008).

**Политика** - общее намерение и направление, официально выраженное руководством (ГОСТ Р ИСО/МЭК 27002-2012).

**Система управления информационной безопасностью (СУИБ)** - часть общей системы управления Институтом, основанная на использовании методов оценки рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности (по ГОСТ Р 53114-2008).

**Система обеспечения информационной безопасности** - совокупность нормативно-правовых, организационных и технических мер по обеспечению защищенности интересов в информационной сфере, а также субъектов информационных отношений.

**Пользователь информационной системы** - лицо, участвующее в функционировании информационной системы либо использующее результаты ее функционирования.

**Правила разграничения доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Ресурс информационной системы** - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Риск** - сочетание вероятности события и его последствий (ГОСТ Р ИСО/МЭК 27002-2012).

**Средства вычислительной техники** - совокупность программных и технических элементов систем обработки информации, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Система защиты информации (данных)** - совокупность организационных и технических мероприятий для защиты информации от неправомерного или случайного доступа, уничтожения, изменения блокирования, копирования, распространения, а также иных неправомерных действий с ней.

**Угрозы безопасности информации (данных)** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать ее уничтожение, изменение, блокирование, копирование, распространение, а также иных несанкционированных действий при ее обработке в информационных системах.

**Уязвимость** - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Приложение №2

к Политике информационной безопасности

ФГБУ «Редакция «Российской газеты»

**Положение**

**О защите от вредоносного программного обеспечения**

**1. Назначение и область действия**

1.1. Настоящее Положение о доступе к информационным ресурсам (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности информационных ресурсов АО ФГБУ «Редакция «Российской газеты» (далее – «Организация») от возможных угроз, которые могут быть связаны с программными воздействиями, разрабатываемым или изменяемым для несанкционированного уничтожения, блокирования, изменения или копирования информации, а также нарушения функционирования элементов информационных систем Организации.

1.2. Соответствует требованиям Политики информационной безопасности Организации.

1.3. Распространяется на всех работников Организации и третьих лиц, использующих информационные ресурсы и системы Организации. Является обязательным для исполнения.

2. Основные требования

2.1. Необходимо установить, настроить и активировать средства защиты от вредоносного программного обеспечения (далее – «ВПО») на всех устройствах, допускающих такую установку, перед началом работы с информационными системами в Организации.

2.2. В Организации допускается использование только лицензионных, свободных или бесплатных средств защиты от ВПО, в соответствии с "Положением об использовании программного обеспечения". Запрещено использовать средства защиты от ВПО без необходимых лицензий или изменять их с целью обхода лицензионных ограничений.

2.3. Процессы установки, настройки, эксплуатации и обновления средств защиты от ВПО должны быть документированы и подвергаться контролю.

2.4. Необходимо разработать список средств защиты от ВПО, чтобы их состав, архитектура и конфигурация могли быть рекомендованы как общее решение для всех подразделений Организации.

2.5. Если программно-технические средства (компьютеры, серверы, коммуникационное оборудование и др.) допускают установку средств защиты от ВПО, но не имеют таковых, то они могут временно отключаться от информационных систем и локальных вычислительных сетей Организации ответственными лицами в случае расследования угроз безопасности, вирусных атак и других инцидентов.

2.6. Средства защиты от ВПО должны всегда иметь актуальные обновления, полученные из доверенных источников.

2.7. Подвергать контролю на предмет обнаружения ВПО следует всю информацию, которая создается или обрабатывается программными средствами, а также информацию, передаваемую через машинные носители или средства связи.

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников Организации и третьих лиц, использующих информационные ресурсы и системы Организации.

3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений Организации; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы Организации; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.