|  |  |  |
| --- | --- | --- |
| |  | | --- | | МИНОБРНАУКИ РОССИИ | | Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА − Российский технологический университет»**  **РТУ МИРЭА** |   **Институт комплексной безопасности и специального приборостроения (ИКБСП)** |
|  |

|  |  |
| --- | --- |
| **ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОЙ РАБОТЫ № 1** | |
|  | |
| Выполнил студент группы БИСО-01-19 | Титов Владислав Андреевич |
|  |

Москва 2020

**Содержание**

[**1. Общие положения** 3](#_Toc54279724)

[**2. Список терминов и определений** 4](#_Toc54279725)

[**3. Область действия** 6](#_Toc54279726)

[**4. Цели и задачи деятельности по обеспечению информационной безопасности** 6](#_Toc54279727)

[**5. Угрозы информационной безопасности** 7](#_Toc54279728)

[**6. Общие требования по обеспечению информационной безопасности** 8](#_Toc54279729)

[**6.1. Ответственность за обеспечение ИБ** 8](#_Toc54279730)

[**6.2. Оценка и обработка рисков** 9](#_Toc54279731)

[**6.3. Контроль доступа** 10](#_Toc54279732)

[**6.4. Управление привилегиями** 11](#_Toc54279733)

[**6.5. Управление паролями** 11](#_Toc54279734)

[**6.6. Контроль прав доступа** 11](#_Toc54279735)

[**6.7. Использование паролей** 11](#_Toc54279736)

[**7. Контроль за соблюдением положений Политики** 12](#_Toc54279737)

# **1. Общие положения**

Политика информационной безопасности ООО “Гора” определяет систему взглядов на проблему обеспечения информационной . Представляет собой систематизированное изложение высокоуровневых целей и задач защиты, которыми необходимо руководствоваться в своей деятельности, а также основных принципов построения системы управления информационной безопасностью Компании.

Обеспечение информационной безопасности – необходимое условие для успешного осуществления уставной деятельности Компании.

Обеспечение информационной безопасности включает в себя любую деятельность, направленную на защиту информационных ресурсов и/или поддерживающей инфраструктуры. Политика охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является Компании.

Реализация Политики должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищённости информационных ресурсов не только с помощью отдельного средства, но и с помощью их простой совокупности. Необходимо их системное, согласованное между собой применение, а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищённом исполнении при оптимальном соотношении технических и организационных мероприятий.

Настоящая политика разработана на основе требований законодательства Российской Федерации, накопленного в Компании опыта в области обеспечения ИБ, интересов и целей Компании. При написании отдельных положений настоящей политики использовались следующие нормативные документы:

* ГОСТ Р ИСО/МЭК 27001 «Методы и средства обеспечения безопасности. Системы

менеджмента информационной безопасности»;

* РС БР ИББС-2.0-2007 «Методические рекомендации по документации в области

обеспечения информационной безопасности…»;

* РС БР ИББС-2.2-2009 «Методика оценки рисков нарушения информационной

безопасности»;

* РС БР ИББС-2.5-2014 «Менеджмент инцидентов информационной безопасности»;
* СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций

банковской системы РФ. Общие положения».

# **2. Список терминов и определений**

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

**Авторизация** – предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ.

**Аутентификация** – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

**Безопасность информации** – защищённость информации от её нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного её тиражирования.

**Бизнес-процесс** – последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности

Учреждения.

**Владелец актива** – физическое или юридическое лицо, которое наделено административной ответственностью за руководство изготовлением, разработкой, хранением, использованием и безопасностью актива. Термин «владелец» не означает, что этот человек фактически имеет право собственности на этот актив.

**Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения** – субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом.

**Документ** – зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать.

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

**Естественные угрозы** — это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека;

**Искусственные угрозы** — это угрозы, вызванные деятельностью человека.

**Защита информации** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и средства доступа к ней.

**Идентификация** – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

**Информация** – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

**Информационная безопасность (ИБ)** – состояние защищённости интересов Учреждения.

**Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**Информационный процесс** – процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

**Информационный ресурс (актив)** – всё, что имеет ценность и находится в распоряжении Учреждения.

**Инцидент** – непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

**Инцидент информационной безопасности** – одно или серия нежелательных, или неожиданных событий ИБ, имеющих значительную вероятность нарушения бизнес-процессов или представляющих угрозу ИБ.

**Коммерческая тайна** – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

**Контролируемая зона** – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.

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

**Конфиденциальность информации** – состояние защищённости информации, характеризуемое способностью ИС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

**Мобильный код** – несамостоятельное программное обеспечение или компонент программного обеспечения (скрипты, макросы, иные компоненты) получаемые из мест распространения мобильного кода, передаваемые по сети и выполняемые на компонентах информационной системы (в местах использования мобильного кода) без предварительной установки (инсталляции) пользователем для расширения возможностей системного и (или) прикладного программного обеспечения.

**Несанкционированный доступ** – доступ к информации иди действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

**Обработка риска** – процесс выбора и реализации мер по модификации (снижению) риска.

**Политика** – общие цели и указания, формально выраженные руководством.

**Привилегии** – это права доверенного объекта на совершение каких-либо действий по

отношению к объектам системы.

**Риск** – сочетание вероятности события и его последствий.

**Система управления информационной безопасностью (СУИБ)** – часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ.

**Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения** – субъект, в полном объёме реализующий полномочия владения, пользования, распоряжения указанными объектами.

**События информационной безопасности** – идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности.

**Угроза** – Опасность, предполагающая возможность потерь (ущерба).

**Целостность информации** – устойчивость информации к несанкционированному доступу или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

# **3. Область действия**

Настоящая Политика распространяется на все бизнес-процессы Компании и обязательна для применения всеми сотрудниками и руководством Компании, а также пользователями его информационных ресурсов. Настоящая политика распространяется на информационные системы учреждения. Лица, осуществляющие разработку внутренних документов Компании, регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой.

# **4. Цели и задачи деятельности по обеспечению информационной безопасности**

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков ИБ. Для достижения основной цели необходимо обеспечивать эффективное решение 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, нормативно методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части ИБ;
* обеспечение непрерывности критических бизнес-процессов;
* достижение адекватности мер по защите от угроз ИБ;
* изучение партнёров, клиентов, конкурентов и кандидатов на работу;
* недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;
* выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников;
* повышение деловой репутации и корпоративной культуры.

# **5. Угрозы информационной безопасности**

Основными источниками угроз безопасности информации являются:

* деятельность преступных групп, экономических структур, а также отдельных лиц по добыванию и/или искажению информации, нарушению работоспособности системы в целом или ее отдельных компонентов;
* воздействия из внутренней сети Компании со стороны сотрудников подразделений Компании, а также удаленное несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (сети Интернет), используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам Компании;
* аварии, стихийные бедствия и прочие форс-мажорные обстоятельства.

Наиболее значимыми угрозами безопасности информации Компании (способами нанесения ущерба субъектам информационных отношений) являются:

* нарушение функциональности компонентов информационной системы Компании, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;
* нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов Компании, а также фальсификация (подделка) документов;
* нарушение конфиденциальности (разглашение, утечка) сведений, составляющих коммерческую тайну, а также персональных данных.

Пользователи, операторы и другие сотрудники Компании являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций, регламентов и порядков.

# **6. Общие требования по обеспечению информационной безопасности**

## **6.1. Ответственность за обеспечение ИБ**

Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в Компании функции обеспечения ИБ возложены на отдел безопасности. На это подразделение возлагается решение следующих основных задач:

* проведение в жизнь Политики ИБ;
* определение требований к защите информации;
* организация мероприятий и координация работ всех подразделений по вопросам комплексной защиты информации;
* контроль и оценка эффективности принятых мер и применяемых средств защиты;
* оказание методической помощи сотрудникам в вопросах обеспечения информационной безопасности;
* регулярная оценка и управление рисками информационной безопасности в соответствии с установленными процедурами в области управления рисками;
* выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения СУИБ;
* обеспечение минимально-необходимого доступа к информационным ресурсам, основываясь на требованиях бизнес-процессов;
* информирование, обучение и повышение квалификации работников Учреждения в сфере информационной безопасности;
* расследования инцидентов информационной безопасности;
* сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности;
* обеспечение необходимого уровня отказоустойчивости ИТ-сервисов и доступности данных для подразделений.

Для решения задач, возложенных на отдел безопасности, его сотрудники имеют следующие

права:

* определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы в указанной области;
* получать информацию от пользователей информационных систем Учреждения по любым аспектам применения информационных технологий в Учреждении;
* участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании и разработке новых информационных технологий;
* участвовать в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации;
* контролировать деятельность пользователей по вопросам обеспечения ИБ;
* готовить предложения руководству по обеспечению требований ИБ.

## **6.2. Оценка и обработка рисков**

В компании должны быть определены требования к безопасности путём методической оценки рисков. Оценки рисков должны выявить, определить количество и расположить по приоритетам риски в соответствии с критериями принятия рисков и бизнес-целями компании.

Результаты оценки должны определять соответствующую реакцию руководства, приоритеты управления рисками ИБ и набор механизмов контроля для защиты от этих рисков. Оценка рисков предполагает системное сочетание анализа рисков и оценивания рисков.

Кроме того, оценка рисков и выбор механизмов контроля должны производиться периодически, чтобы:

* учесть изменения бизнес-требований и приоритетов;
* принять во внимание новые угрозы и уязвимости;
* убедиться в том, что реализованные средства сохранили свою эффективность.

Перед обработкой каждого риска Компании должно выбрать критерии для определения возможности принятия этого риска. Риск может быть принят, если его величина достаточно мала и стоимость обработки нерентабельна для Компании. Такие решения должны регистрироваться.

Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

* применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня;
* сознательное и объективное принятие риска, если он точно удовлетворяет Политике Компании и критериям принятия рисков;
* уклонение от риска путём недопущения действий, могущих быть его причиной;
* передача рисков другой стороне (аутсорсинг, страхование и т.п.).

## **6.3. Контроль доступа**

Основными пользователями информации в информационной системе Компании являются сотрудники структурных подразделений. Уровень полномочий каждого пользователя определяется индивидуально. Каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями.

Допуск пользователей к работе с информационными ресурсами должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться в установленном порядке, согласно регламенту предоставления доступа пользователей.

Каждому пользователю, допущенному к работе с конкретным информационным активом Компании, должно быть сопоставлено персональное уникальное имя (учётная запись пользователя), под которым он будет регистрироваться и работать с ИА.

В случае производственной необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имён (учётных записей).

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

В общем случае запрещено создавать и использовать общую пользовательскую учётную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учётной записи должно сопровождаться отметкой в журнале учёта машинного времени, которая должна однозначно идентифицировать текущего владельца учётной записи в каждый момент времени. Одновременное использование одной общей пользовательской учётной записи разными пользователями запрещено.

Регистрируемые учётные записи подразделяются на:

* Пользовательские – предназначенные для аутентификации пользователей ИР Компании;
* Системные – используемые для нужд операционной системы;
* Служебные – предназначенные для функционирования отдельных процессов или приложений.

Системные учётные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные учётные записи используются только для запуска и работы сервисов или приложений.

Использование системных или служебных учётных записей для регистрации пользователей в системе категорически запрещено.

Процедуры регистрации и блокирования учётных записей пользователей должны применяться с соблюдением следующих правил:

* использование уникальных идентификаторов (ID) пользователей для однозначного определения и сопоставления личности с совершёнными ей действиями;
* использование групповых ID разрешать только в случае, если это необходимо для выполнения задачи;
* предоставление и блокирование прав должны быть санкционированы и документированы;
* предоставление прав доступа к ИР, только после согласования с владельцем данного ИР;
* регистрация и блокирование учётных записей допускается с отдельного разрешения руководства Учреждения;
* уровень предоставленных полномочий должен соответствовать производственной необходимости и настоящей Политике и не ставить под угрозу разграничение режимов работы;
* согласование изменения прав доступа с отделом ИС СМТ;
* документальная фиксация назначенных пользователю прав доступа;
* ознакомление пользователей под подпись с письменными документами, в которых регламентируются их права доступа;
* предоставление доступа с момента завершения процедуры регистрации;
* обеспечение создания и поддержания формального списка всех пользователей, зарегистрированных для работы с ИР или сервисом;
* немедленное удаление или блокирование прав доступа пользователей, сменивших должность, форму занятости или уволившихся из Учреждения;
* аудит ID и учетных записей пользователей на наличие неиспользуемых, их удаление и блокировка;
* обеспечение того, чтобы лишние ID пользователей не были доступны другим пользователям;
* обеспечить возможность предоставления пользователям доступа в соответствии с их должностями, основанными на производственных требованиях, путем суммирования некоторого числа прав доступа в типовые профили доступа пользователей.

## **6.4. Управление привилегиями**

## **6.5. Управление паролями**

## **6.6. Контроль прав доступа**

## **6.7. Использование паролей**

# **7. Контроль за соблюдением положений Политики**

Общий контроль состояния ИБ Учреждения осуществляется Директором.

Текущий контроль соблюдения настоящей Политики осуществляет отдел ИС СМТ. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов ИБ Учреждения, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

Отдел ИС СМТ ежегодно пересматривает положения настоящей политики. Изменения и дополнения вносятся по инициативе отдела ИС СМТ или Директора и утверждаются Директором.

Порядок пересмотра документов второго и третьего уровней определяется в данных документах.

Все изменения, внесённые в настоящую Политику ИБ должны учитываться в листе «История изменений».