Утверждаю:
Генеральный директор
ООО «Магистраль»
_____Л.В.Хайбуллин
«12» 04 2022г.

Политика информационной безопасности в ООО «Магистраль»

1. Общие положения

Политика информационной безопасности (далее–Политика) в ООО Магистраль (далее Общество) определяет систему взглядов на проблему обеспечения информационной безопасности (далее–ИБ). Представляет собой систематизированное изложение высокоуровневых целей и задач защиты, которыми необходимо руководствоваться в своей деятельности, а также основных принципов построения системы управления информационной безопасностью (далее–СУИБ) в Обществе.

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

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 Общество.

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.

2. Обозначения и сокращения

ИБ - информационная безопасность
ИР - информационный ресурс
ИС - информационная система
ИТ - информационные технологии
ПК - персональный компьютер
ПО - программное обеспечение
СКЗИ - средство криптографической защиты информации
СУИБ - система управления информационной безопасностью

3. Термины и определения

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 Общества.

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.

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 Общества.

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 Общества.

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.

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.

4. Цель

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. Основания для разработки

Настоящая политика разработана на основе требований законодательства Российской Федерации, накопленного в Обществе опыта в области обеспечения ИБ, интересов и целей Общества.

При написании отдельных положений настоящей политики использовались следующие нормативные документы:

- ГОСТ Р ИСО/МЭК27001«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».

6. Область действия

Настоящая Политика распространяется на все бизнес-процессы Общества и обязательна для применения всеми сотрудниками.

Настоящая политика распространяется на информационные системы Общества.

Лица, осуществляющие разработку внутренних документов Общества, регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой.

7. Содержание политики

7.1. Система управления информационной безопасностью.

Для достижения указанных целей и задач в Обществе внедряется система управления информационной безопасностью.

СУИБ документирована в настоящей политике, в правилах, процедурах, рабочих инструкциях, которые являются обязательными для всех работников Общества в области действия системы. Документированные требования СУИБ доводятся до сведения работников Общества.

Средства управления информационной безопасностью внедряются по результатам проведения оценки рисков информационной безопасности.

Стоимость внедряемых средств управления информационной безопасностью не должна превышать возможный ущерб, возникающий при реализации угроз.

7.1.1. Структура документов

В целях создания взаимосвязанной структуры нормативных документов Общества в области обеспечения информационной безопасности, разрабатываемые и обновляемые нормативные документы должны соответствовать следующей иерархии:

- настоящая Политика является внутренним нормативным документом по ИБ первого уровня.
- документы второго уровня – инструкции, порядки, регламенты и прочие документы, описывающие действия сотрудников Общества по реализации документов первого и второго уровня.
- документы третьего уровня – отчётные документы о выполнении требований документов верхних уровней.

7.1.2. Ответственность за обеспечение ИБ

Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в Обществе функции обеспечения ИБ возложены на генерального директора. На него 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 и обучение работников Общества 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 решения этих задач он имеет следующие права:

- определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы;

- получать информацию от пользователей информационных систем Общества по любым аспектам применения информационных технологий в Обществе;
- 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;

7.2. Объект защиты

7.2.1. Ответственность за ресурсы

В Обществе должны быть выявлены и оценены с точки зрения их важности все ресурсы. Для всех ценных ресурсов должен быть составлен реестр (перечень). Благодаря информации о ресурсах Общества реализуется защита информации, степень которой соразмерна ценности и важности ресурсов.

В ИС Общества присутствуют следующие типы ресурсов:

- информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности Общества;
- открыто распространяемая информация, необходимая для работы Общества, независимо от формы и вида её представления;
- информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Владельцем всех ресурсов является генеральный директор. Он отвечает за соответствующую классификацию информации и ресурсов, связанных со средствами обработки информации, а также за назначение и периодическую проверку прав доступа и категорий, определённых политиками управления доступа.

7.2.2. Классификация информации

Все информационные ресурсы, подлежащие защите, должны быть классифицированы в соответствии с важностью и степенью доступа. Классификация информации должна быть документирована и утверждена генеральным директором. Классификация информации проводится генеральным директором. Периодически классификация должна пересматриваться для поддержания актуальности её соответствия с категорией ресурса.

Ресурсы, содержащие конфиденциальную или критичную информацию, должны иметь соответствующую пометку (гриф).

7.3. Оценка и обработка рисков

В Обществе 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 учреждения. Результаты оценки должны определять 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 Общество должно выбрать критерии для определения возможности принятия этого риска. Риск может быть принят, если его величина достаточно мала и стоимость обработки нерентабельна для Общества.
- 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 Общества и критериям принятия рисков;
- уклонение от риска путём недопущения действий, которые могут быть его причиной;
- передача рисков другой стороне (аутсорсинг, страхование и т.п.).

7.4. Безопасность персонала

Роли и обязанности по обеспечению безопасности информационных ресурсов, описанные в соответствии с Политикой ИБ Общества, должны быть доведены до сотрудника при трудоустройстве и внесены в его должностные обязанности. Сюда должны входить как общие обязанности по реализации и поддержке политики безопасности, так и конкретные обязанности по защите ресурсов и по выполнению конкретных операций, связанных с безопасностью.

7.4.1. Условия найма

Все принимаемые на работу сотрудники должны одобрить и подписать свои трудовые договоры, в которых устанавливается их ответственность за ИБ. В договор должно быть включено согласие сотрудника на проведение контрольных мероприятий со стороны Общества по проверке выполнения требований ИБ, а также обязательства по неразглашению конфиденциальной информации. В договоре должны быть описаны меры, которые будут приняты в случае несоблюдения сотрудником требований ИБ.

Обязанности по обеспечению ИБ должны быть включены в должностные инструкции каждого сотрудника Общества.

Все принимаемые сотрудники должны быть ознакомлены под роспись с перечнем информации, ограниченного доступа, с установленным режимом с ней и с мерами ответственности за нарушение этого режима.

При предоставлении сотруднику доступа к ИС Общества он должен ознакомиться под роспись с инструкцией пользователя ИС.

7.4.2. Ответственность руководства

Руководство Общества должно требовать от всех сотрудников, подрядчиков и пользователей сторонних организаций принятия мер безопасности в соответствии с установленными в Обществе политиками и процедурами.

Уполномоченные руководством Общества сотрудники имеют право в установленном порядке, без уведомления пользователей, производить проверки:

- выполнения действующих инструкций по вопросам ИБ;
- данных, находящихся на носителях информации;
- порядка использования сотрудниками информационных ресурсов;
- содержания служебной переписки.

7.4.3. Обучение ИБ

Все сотрудники должны проходить периодическую подготовку в области политики и процедур ИБ, принятых в Обществе.

7.4.4. Завершение или изменения трудовых отношений

При увольнении все предоставленные сотруднику права доступа к ресурсам ИС должны быть удалены. При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых отношениях.

7.5. Физическая безопасность

7.5.1. Защищённые области

Средства обработки информации, поддерживающие критически важные и уязвимые ресурсы Общества, должны быть размещены в защищённых областях. Такими средствами являются: серверы, оборудование, обеспечивающее обработку и хранение конфиденциальной информации.

Защищённые области должны быть под контролем, ограничивающим доступ посторонних лиц.

Для хранения служебных документов и машинных носителей с защищаемой информацией помещение снабжается сейфами, металлическими шкафами или шкафами, оборудованными замком.

Помещение должно быть обеспечено средствами уничтожения документов.

7.5.2. Области общего доступа

Места доступа, через которые посторонние лица могут попасть в помещение Общества, должны контролироваться с целью предотвращения несанкционированного доступа.

7.5.3. Вспомогательные службы

Все вспомогательные службы, такие как электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха должны обеспечивать гарантированную и устойчивую работоспособность компонентов ИС Общества.

7.5.4. Утилизация или повторное использование оборудования

Со всех носителей информации, которыми укомплектовано утилизируемое оборудование, должны гарантированно удаляться все конфиденциальные данные и лицензионное ПО.

7.5.5. Перемещение имущества

Оборудование, информация или ПО не должны перемещаться за пределы Общества без ведома руководства.

7.6. Контроль доступа

Основными пользователями информации в информационной системе Общества являются сотрудники. 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.

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

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).

Запрещено создавать и использовать общую пользовательскую учётную запись для группы пользователей.

Регистрируемые учётные записи подразделяются на:

- пользовательские–предназначенные для аутентификации пользователей ИР общества;
- 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 на сервере 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 определяется исключительно генеральным директором;
- регистрация и блокирование учётных записей допускается исключительно генеральным директором;
- уровень предоставленных полномочий должен соответствовать производственной необходимости и настоящей Политике и не ставить под угрозу разграничение режимов работы;
- немедленное удаление или блокирование прав доступа пользователей, сменивших должность, форму занятости или уволившихся из Общества;
- аудит ID и учетных записей пользователей на наличие неиспользуемых, их удаление и блокировка;
- обеспечение того, чтобы лишние ID пользователей не были доступны другим пользователям;

7.6.1. Управление паролями

Пароли – средство проверки личности пользователя для доступа к ИС, обеспечивающее идентификацию и аутентификацию.

Предоставление паролей должно контролироваться посредством официальной процедуры, отвечающей следующим требованиям:

- все пользователи должны быть ознакомлены под роспись с требованием сохранения в тайне личных и групповых паролей;
- необходимо избегать передачи паролей с использованием третьих лиц или незашифрованной электронной почтой;
- пароли должны храниться в электронном виде только в защищенной форме;
- необходимо установить требования к длине пароля и набору символов;
- необходимо изменять пароль пользователя не реже одного раза в 90 дней.

7.6.2. Контроль прав доступа

Контроль над выполнением процедур управления доступом пользователей должен включать:

- контроль над добавлением, удалением и изменением идентификаторов, аутентификационных данных и иных объектов идентификации;
- немедленное блокирование прав доступа при увольнении;
- включение учётных записей, используемых поставщиками для удалённой поддержки, только на время выполнения работ;
- отслеживание удалённых учётных записей, используемых поставщиками, во время работ;
- использование механизмов аутентификации при доступе к любой базе данных, содержащей сведения ограниченного распространения, в том числе доступе со стороны приложений, администраторов и любых других пользователей;
- разрешение запросов и прямого доступа к базам данных только для администраторов баз данных;
- блокирование учетных записей пользователей при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены оператором к событиям нарушения безопасности информации.

7.6.3. Использование паролей

Идентификатор и пароль пользователя в ИС являются учётными данными, на основании которых сотруднику Общества предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой и хранимой) сотрудником информации.

Не допускается использование различными пользователями одних и тех же учётных данных.

Значение пароля учетной записи пользователя устанавливает генеральный директор.

Личные пароли устанавливаются с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля должны присутствовать три из четырёх видов символов:

1. буквы в верхнем регистре;
2. буквы в нижнем регистре;
3. цифры;
4. специальные символы (!@#$%^&*()-_+=~[]{}|\:;'"<>,.?/);

- пароль не должен содержать легко вычисляемые сочетания символов, например:

1. имена, фамилии, номера телефонов, даты;
2. последовательно расположенные на клавиатуре символы («12345678», «QWERTY», и т.д.);
3. общепринятые сокращения («USER», «TEST» и т.п.);

4. повседневно используемое слово, например, имена или фамилии друзей, коллег, актёров или сказочных персонажей, клички животных;
5. компьютерный термин, команда, наименование компаний, web-сайтов, аппаратного или программного обеспечения;
6. что-либо из вышеперечисленного в обратном написании;
7. что-либо из вышеперечисленного с добавлением цифр в начале или конце;
8. при смене пароля значение нового должно отличаться от предыдущего не менее чем в 4 позициях;
9. для различных ИС необходимо устанавливать собственные, отличающиеся пароли.

Сотруднику рекомендуется выбирать пароль с помощью следующей процедуры:

1. выбрать фразу, которую легко запомнить. Например, «Три мудреца в одном тазу пустились по морю в грозу»;
2. выбрать первые буквы из каждого слова «тмвотппмвг»;
3. набрать полученную последовательность, переключившись на английскую раскладку клавиатуры: «nvdjnggvdu»;
4. выбрать номер символа, который будет записываться в верхнем регистре и после которого будет специальный символ. Например, это будет пятый символ, а в качестве специального символа выбран «#». Получаем: «nvdjN#ggvdu».

Сотруднику запрещается:

- сообщать свой пароль кому-либо;
- указывать пароль в сообщениях электронной почты;
- хранить пароли, записанные на бумаге, в легко доступном месте;
- использовать тот же самый пароль, что и для других систем (например, домашний интернет-провайдер, бесплатная электронная почта, форумы и т.п.);
- использовать один и тот же пароль для доступа к различным корпоративным ИС.

Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место пользователь обязан заблокировать компьютер (используя комбинации Win+L или Ctrl+Alt+Delete→ «Блокировать компьютер»).

Сотрудник обязан:

- в случае подозрения на то, что пароль стал кому-либо известен, поменять пароль и сообщить об этом генеральному директору;
- немедленно сообщить директору случае получения от кого-либо просьбы сообщить пароль;
- менять пароль каждые 90 дней;
- менять пароль по требованию генерального директора;
- Учреждение оставляет за собой право:
- осуществлять периодическую проверку стойкости паролей пользователей, используемых сотрудниками для доступа к ИС;
- принимать меры дисциплинарного характера к сотрудникам, нарушающим положения настоящей политики.

7.6.4. Пользовательское оборудование, оставляемое без присмотра

Пользователи должны обеспечивать необходимую защиту оборудования, остающегося без присмотра. Все пользователи должны быть осведомлены о требованиях ИБ и правилах защиты остающегося без присмотра оборудования, а также о своих обязанностях по обеспечению этой защиты.

7.6.5. Политика чистого стола

Сотрудники Общества обязаны:

- сохранять известные им пароли в тайне;
- закрывать активные сеансы по завершении работы, если только их нельзя защитить подходящим блокирующим механизмом, например, защищённый паролем хранитель экрана;
- по завершении сеанса выходить из системы офисных ПК.

Запрещается вести запись паролей (например, на бумаге, в программном файле или в карманном устройстве).

Документы и носители с конфиденциальной информацией должны убираться в запираемые места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места.

Компьютеры должны быть оставлены в состоянии выполненного выхода из системы, когда они находятся без присмотра.

Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место, пользователь обязан заблокировать компьютер (используя комбинации Win+L или Ctrl+Alt+Delete→ «Блокировать компьютер»).

Документы, содержащие конфиденциальную информацию, должны изыматься из печатающих устройств немедленно.

В конце рабочего дня сотрудник должен привести в порядок письменный стол и убрать все офисные документы в запираемый шкаф или сейф.

Для утилизации конфиденциальных документов, должны использоваться уничтожители бумаги.

По окончании рабочего дня и в случае длительного отсутствия на рабочем месте необходимо запирать на замок все шкафы и сейфы.

7.6.6. Мобильное компьютерное оборудование

При использовании мобильных средств (например, ноутбуков, планшетов и мобильных телефонов) необходимо соблюдать особые меры предосторожности, чтобы не допустить компрометацию информации, принадлежащей Общества. Необходимо принять официальную политику, учитывающую риск, связанный с использованием мобильных компьютеров, и, в частности, с работой в незащищённой среде.

7.7. Политика допустимого использования информационных ресурсов

Общие обязанности пользователя:

- при работе с ПО руководствоваться нормативной документацией (руководством пользователя);
- обращаться в службу поддержки пользователей или к специалистам, назначенным и ответственными за системное администрирование и информационную безопасность, по всем техническим вопросам, связанным с работой в корпоративной ИС (подключение к корпоративной ИС/домену, инсталляция и настройка ПО, удаление вирусов, предоставление доступа в сеть Интернет и к внутренним сетевым ресурсам, ремонт и техническое обслуживание и т.п.),а так же за необходимой методологической/консультационной помощью по вопросам применения технических и программных средств корпоративной ИС;

- знать признаки правильного функционирования установленных программных продуктов и средств защиты информации;
- минимизировать вывод на печать обрабатываемой информации.

7.7.1. Использование ПО

На офисных ПК и серверах допускается использование только лицензионного программного обеспечения.

Запрещено незаконное хранение на жестких дисках офисных ПК информации, являющейся объектом авторского права (ПО, фотографии, музыкальные файлы, игры, и т.д.).

Решение о приобретении и установке программного обеспечения принимается непосредственно генеральным директором.

Документы, подтверждающие покупку программного обеспечения, хранятся в бухгалтерии на протяжении всего времени использования лицензии, копии указанных документов вместе с лицензионными соглашениями на ПО, ключами защиты ПО и дистрибутивами хранятся у генерального директора.

Пользователи офисных ПК не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию на офисных ПК. Указанные работы, а также работы по установке, регистрации и активации приобретённого лицензионного ПО могут быть выполнены только генеральным директором.

7.7.2. Использование офисных ПК и ИС

К работе в ИС Общества допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам информационной безопасности.

Ответственность по установке и поддержке всех компьютерных систем, функционирующих в Общества, возложена на генерального директора.

Каждый сотрудник Общества, обеспеченный офисным ПК, получает персональное сетевое имя, пароль, адрес электронной почты и личный каталог в сети, который предназначен для хранения рабочих файлов.

Работа в ИС сотрудникам разрешена только на закреплённых за ними ПК, в определённое время и только с разрешенным программным обеспечением и сетевыми ресурсами.

Все ПК, установленные в Обществе, имеют унифицированный набор офисных программ, предназначенных для получения, обработки и обмена информацией, определённый в стандарте рабочих мест Общества. Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется генеральным директором.

Самостоятельная установка программного обеспечения на ПК запрещена. Установка и удаление любого программного обеспечения производится только генеральным директором (по указанию генерального директора, специалистом).

В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться напрямую к генеральному директору.

Генеральный директор имеет право осуществлять контроль над установленным на компьютере программным обеспечением, и принимать меры по ограничению возможностей несанкционированной установки программ.

Передача документов внутри Общества производится только посредством общих папок, а также средствами электронной почты.

При работе в ИС Общества сотрудник обязан:

- знать и выполнять требования внутренних организационно-распорядительных документов Общества;
- использовать ИС и ПК Общества исключительно для выполнения своих служебных обязанностей;
- ставить в известность генерального директора о любых фактах нарушения требований ИБ;
- ставить в известность генерального директора о любых фактах сбоев ПО, некорректного завершения значимых операций, а также повреждения технических средств;
- незамедлительно выполнять предписания генерального директора;
- Предоставлять ПК генеральному директору для контроля;
- При необходимости прекращения работы на некоторое время корректно закрывать все активные задачи, блокировать ПК;
- В случае необходимости продолжения работы по окончании рабочего дня проинформировать об этом генерального директора.
- При использовании ИС Общества запрещено:
- использовать ПК и ИС в личных целях;
- отключать средства управления и средства защиты, установленные на рабочей станции;
- передавать:

1. конфиденциальную информацию за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с генеральным директором;
2. информацию, файлы или ПО, способные нарушить или ограничить функциональность любых программных и аппаратных средств, а также ссылки на вышеуказанные объекты;
3. угрожающую, клеветническую, непристойную информацию;

- самовольно вносить изменения в конструкцию, конфигурацию, размещение ПК и других узлов ИС Общества;
- предоставлять сотрудникам Общества (за исключением генерального директора) и третьим лицам доступ к своему ПК;
- запускать на ПК ПО, не входящее в Реестр разрешенного к использованию ПО;
- самостоятельно подключать рабочую станцию и прочие технические средства к корпоративной ИС Общества;
- осуществлять поиск средств и путей повреждения, уничтожения технических средств и ресурсов ИС или осуществлять попытки несанкционированного доступа к ним;

Все электронные сообщения и документы в электронном виде, передаваемые посредством ИС Учреждения подлежат обязательной проверке на отсутствие вредоносного ПО.

7.7.3. Использование ресурсов локальной сети

Для выполнения своих служебных обязанностей каждый сотрудник обеспечивается доступом к соответствующим информационным ресурсам. Информационными ресурсами являются каталоги и файлы, хранящиеся на дисках серверов Общества, базы данных, электронная почта.

Основными рабочими каталогами являются личные каталоги сотрудников и каталоги подразделений, созданные в соответствии с особенностями их работы. Доступ сотрудников к ресурсам сети осуществляется согласно матрице доступа. Временное расширение прав доступа осуществляется генеральным директором.

7.7.4. Обработка конфиденциальной информации

При обработке конфиденциальной информации сотрудники обязаны:

- знать и выполнять требования Инструкции по работе с конфиденциальной информацией;
- при необходимости размещать конфиденциальную информацию на открытом ресурсе корпоративной сети Общества применять средства защиты от неавторизованного доступа;
- размещать экран монитора таким образом, чтобы исключить просмотр обрабатываемой информации посторонними лицами;
- не отправлять на печать конфиденциальные документы, если отсутствует возможность контроля вывода на печать и изъятия отпечатанных документов из принтера сразу по окончании печати;
- обязательно проверять адреса получателей электронной почты на предмет правильности их выбора;
- не запускать исполняемые файлы на съемных накопителях, полученные не из доверенного источника;
- не передавать конфиденциальную информацию по открытым каналам связи, кроме сетей корпоративной ИС;
- не оставлять без личного присмотра на рабочем месте или где бы то ни было электронные носители информации (CD/DVD–диски, Flash–устройства и пр.), а также распечатки из принтера или бумажные копии документов, содержащие конфиденциальную информацию.

7.7.5. Использование электронной почты

Электронная почта используется для обмена в рамках ИС Общества и общедоступных сетей информацией в виде электронных сообщений и документов в электронном виде.

Для обеспечения функционирования электронной почты допускается применение ПО, входящего в реестр разрешённого к использованию ПО.

При работе с корпоративной электронной почтой Общества пользователь должен учитывать:

- электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;
- электронная почта не является средством передачи информации, гарантирующим конфиденциальность передаваемой информации (передачу конфиденциальной информации вне локальной сети Общества необходимо осуществлять только в зашифрованном виде);
- электронная почта не является средством передачи информации, гарантированно идентифицирующим отправителя сообщения.

Организацией и обеспечением порядка работы электронной почты в Обществе занимается директор.

Адрес электронной почты и пароль выдаёт непосредственно генеральный директор.

Любые сообщения электронной почты могут быть прочитаны, использованы в интересах Общества либо удалены генеральным директором.

Пользователям электронной почты Общества запрещено вести частную переписку с использованием средств электронной почты Общества. К частной переписке относится переписка, не связанная с исполнением сотрудником своих должностных обязанностей.

Использование электронной почты Общества для частной переписки сотрудником, надлежащим образом, ознакомленным с данной Политикой, является нарушением трудовой дисциплины Общества. Подписываясь в ознакомлении с настоящей Политикой, сотрудник даёт согласие на

ознакомление и иное использование в интересах Общества его переписки, осуществляемой с использованием электронной почты, и соглашается с тем, что любое использование его переписки, осуществляемой с использованием электронной почты, не может рассматриваться как нарушение тайны связи.

Каждый сотрудник Общества имеет право на просмотр либо иное использование в интересах Общества сообщений электронной почты, которые направлены или получены им, соответственно, с или на электронный адрес Общества.

Исходящие электронные сообщения сотрудников Общества должны содержать следующие поля:

- адрес получателя;
- тема электронного сообщения;
- текст электронного сообщения (вложенные файлы);
- подпись отправителя;
- предупреждение о служебном характере сообщения и его конфиденциальности.

Формат подписи отправителя:

С уважением, <Фамилия имя>

<Должность> <Структурное подразделение> <Наименование Общества> <Адрес>

<номера контактов: телефон, мессенджеры, адреса электронной почты> <сайт>

Формат предупреждения о служебном характере сообщения и его конфиденциальности:

«Это электронное сообщение и любые документы, приложенные к нему, содержат конфиденциальную информацию. Настоящим уведомляем Вас о том, что, если это сообщение не предназначено Вам, использование, копирование, распространение информации, содержащейся в настоящем сообщении, а также осуществление любых действий на основе этой информации, строго запрещено и защищается законодательством Российской Федерации. Если Вы получили это сообщение по ошибке, пожалуйста, сообщите об этом отправителю по электронной почте и удалите это сообщение. CONFIDENTIALITY NOTICE: This email and any files attached to it are confidential. If you are not the intended recipient you are notified that using, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited and protected by the laws of the Russian Federation. If you have received this email in error, please notify the sender and delete this email. »

При формировании ответов на полученные электронные сообщения можно использовать следующую упрощённую подпись:

С уважением,

<Фамилия имя> <Номера телефонов, мессенджеры, адреса электронной почты>

В случае получения служебного сообщения о невозможности доставки сообщения адресату или получения извещения от адресата о том, что он не получил отправленное ему сообщение, необходимо сообщить об этом генеральному директору.

Отказ от дальнейшего предоставления сотруднику Общества услуг электронной почты может быть вызван нарушениями требований настоящей политики.

Прекращение предоставления сотруднику Общества услуг электронной почты наступает при прекращении действия трудового договора (контракта) сотрудника.

7.7.6. Работа в сети

Доступ к сети Интернет предоставляется сотрудникам Общества в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

Для доступа сотрудников Общества к сети Интернет допускается применение ПО, входящего в Реестр разрешённого к использованию ПО.

При использовании сети Интернет необходимо:

- соблюдать требования настоящей Политики;
- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
- ставить в известность директора о любых фактах нарушения требований настоящей Политики;
- При использовании сети Интернет запрещено:
- использовать предоставленный Обществом доступ в сеть Интернет в личных целях;
- использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;
- совершать любые действия, направленные на нарушение нормального функционирования элементов ИС Учреждения;
- публиковать, загружать и распространять материалы, содержащие:

1. Конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным;
2. угрожающую, клеветническую, непристойную информацию;
3. вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также ссылки на него;
4. фальсифицировать свой IP-адрес, а также прочую служебную информацию.

Учреждение оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством.

Информация о посещаемых сотрудниками Общества Интернет-ресурсах может протоколироваться для последующего анализа.

Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

7.7.7. Использование мобильных устройств

Под использованием мобильных устройств и носителей информации в ИС Общества понимается их подключение к инфраструктуре ИС с целью обработки, приёма/передачи информации между ИС и мобильными устройствами, а также носителями информации.

На предоставленных Обществом мобильных устройствах допускается использование ПО, входящего в Реестр разрешённого к использованию ПО.

К предоставленным Обществом мобильным устройствам и носителям информации предъявляются те же требования ИБ, что и для стационарных ПК. Целесообразность дополнительных мер обеспечения ИБ определяется директором.

7.7.8. Защита от вредоносного ПО

Генеральный директор регулярно проверяет сетевые ресурсы Общества антивирусным программным обеспечением и обеспечивает защиту входящей электронной почты от проникновения вирусов и другого вредоносного ПО.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление о системных ошибках, увеличение исходящего/входящего трафика и т.п.) сотрудник Общества должен незамедлительно оповестить об этом генерального директора. После чего генеральный директор должен провести внеочередную полную проверку на вирусы рабочей станции пользователя, проверив, в первую очередь, работоспособность антивирусного ПО.

В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения заражения директора, а также других сотрудников, использующих эти файлы в работе.
- совместно с директором провести анализ необходимости дальнейшего их использования.
- для предупреждения вирусного заражения рекомендуется:
- никогда не открывать файлы и не выполнять макросы, полученные в почтовых сообщениях от неизвестного или подозрительного отправителя.
- удалять подозрительные вложения, не открывая их, и очищать корзину, где хранятся удаленные сообщения;
- удалять спам, рекламу и другие бесполезные сообщения;
- никогда не загружать файлы и программное обеспечение из подозрительных или неизвестных источников;

периодически резервировать важные данные и системную конфигурацию, хранить резервные копии в безопасном месте.

7.8. Приобретение, разработка и обслуживание систем

7.8.1. Требования безопасности для информационных систем

При описании требований к созданию новых систем или к усовершенствованию существующих необходимо учитывать потребность в средствах обеспечения безопасности.

Требования к безопасности и средства защиты должны соответствовать ценности используемых ИР и потенциальному ущербу для Общества в случае сбоя или нарушения безопасности. Основой для анализа требований к безопасности и выбору мер для поддержки безопасности является оценка рисков и управление рисками.

Системные требования к ИБ и процессам, обеспечивающим защиту информации, должны быть включены на ранних стадиях проектирования ИС.

7.8.2. Корректная обработка информации

Данные, вводимые в прикладные системы, необходимо проверять, чтобы гарантировать их правильность и соответствие поставленной задаче.

7.8.3. Криптографические средства

Все, поступающие в Обществе, СКЗИ должны быть учтены в соответствующем журнале учёта СКЗИ.

В Обществе должно осуществляться управление ключами для эффективного применения криптографических методов. Компрометация или потеря криптографических ключей может привести к нарушению конфиденциальности, подлинности и/или целостности информации.

Все ключи должны быть защищены от изменения, утери и уничтожения. Кроме того, секретные и закрытые ключи должны быть защищены от несанкционированного раскрытия. Оборудование, используемое для генерации, хранения и архивирования ключей должно быть физически защищено.

Соглашения с внешними поставщиками криптографических услуг (например, удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса.

Криптографические системы и методы следует использовать для защиты конфиденциальной информации, когда другие средства контроля не обеспечивают адекватной защиты.

Для критической информации должно использоваться шифрование при их хранении в базах данных или передаче по коммерческим или открытым сетям, таким как Интернет.

7.8.3.1. Требований по обеспечению ИБ при использовании СКЗИ

Шифрование – это криптографический метод, который может использоваться для обеспечения защиты конфиденциальной, важной или критичной информации.

СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения.

Порядок применения СКЗИ определяется руководством Общества и должен включать:

- порядок ввода в действие, включая процедуры встраивания СКЗИ в ИС;
- порядок эксплуатации;
- порядок восстановления работоспособности в аварийных случаях;
- порядок внесения изменений;
- порядок снятия с эксплуатации;
- порядок управления ключевой информацией;
- порядок обращения с ключевой информацией, включая действия при смене и компрометации ключей.

Для шифрования конфиденциальной информации минимально допустимой длинной ключа является 128 бит.

При использовании шифрования в ИС Общества должны применяться только утверждённые стандартные алгоритмы и сертифицированные ФСБ России продукты, их реализующие.

7.8.3.2. Электронные цифровые подписи

ЭЦП обеспечивают защиту аутентификации и целостности электронных документов.

ЭЦП могут применяться для любой формы документа, обрабатываемого электронным способом. ЭЦП должны быть реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой–для проверки подписи (открытый ключ).

Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой, имеющий к нему доступ, может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Защиты целостности открытого ключа должна обеспечиваться при использовании сертификата открытого ключа.

Криптографические ключи, используемые для цифровых подписей, должны отличаться от тех, которые используются для шифрования.

При использовании ЭЦП, необходимо учитывать требования действующего законодательства Российской Федерации, определяющего условия, при которых цифровая подпись имеет юридическую силу.

7.8.3.3. Управление ключами

Управление криптографическими ключами важно для эффективного использования криптографических средств.

Любая компрометация или потеря криптографических ключей может привести к компрометации конфиденциальности, подлинности и/или целостности информации. Следует применять систему защиты для обеспечения использования в ИС Общества криптографических методов в отношении открытых ключей, где каждый пользователь имеет пару ключей, открытый ключ (который может быть показан любому) и личный ключ (который должен храниться в секрете). Методы с открытыми ключами должны использоваться для шифрования и для генерации цифровых подписей.

Ключи необходимо защищать от изменения и разрушения, а секретным и личным ключам необходима защита от неавторизованного раскрытия. Криптографические методы могут также использоваться для этой цели. Физическую защиту следует применять для защиты оборудования, используемого для изготовления, хранения и архивирования ключей.

Для безопасного взаимодействия с внешними пользователями ИС Общества необходимо использовать электронные сертификаты только из утверждённого списка сертифицированных центров.

Секретные ключи пользователей должны храниться так же, как и пароли. О любом подозрении на компрометацию секретного ключа пользователь должен немедленно доложить генеральному директору.

Необходимо, чтобы система обеспечения безопасности использования ключей основывалась на согласовании способов, процедур и безопасных методов для:

- генерации ключей при использовании различных криптографических систем и приложений;
- генерации и получения сертификатов открытых ключей;
- рассылки ключей, предназначенных пользователям, включая инструкции по их активации при получении;
- хранения ключей (при этом необходимо наличие инструкции авторизованным пользователям для получения доступа к ключам);
- смены или обновления ключей, включая правила порядка и сроков смены ключей;
- порядка действий в отношении скомпрометированных ключей;
- аннулирования ключей, в том числе способы аннулирования или дезактивации ключей, если ключи были скомпрометированы или пользователь уволился из организации (в этом случае ключи необходимо архивировать);
- восстановление ключей, которые были утеряны или испорчены, для рассекречивания зашифрованной информации;
- архивирования и резервного копирования ключей;
- разрушения ключей;
- регистрация ключей и аудита действий, связанных с управлением ключами.

Для уменьшения вероятности компрометации, для ключей необходимо определить даты начала и конца действия, чтобы их можно было использовать лишь в течении ограниченного периода

времени, который зависит от обстоятельств использования криптографических средств, контроля и от степени риска раскрытия информации.

Может потребоваться наличие процедур обработки юридических запросов, касающихся доступа к криптографическим ключам, например, чтобы зашифрованная информация стала доступной в незашифрованном виде для доказательств в суде.

Необходимо обеспечивать защиту открытых ключей от угроз подделывания цифровой подписи и замены открытого ключа пользователя своим. Эта проблема решается с помощью сертификата открытых ключей. Сертификаты необходимо изготавливать таким способом, который однозначно связывал бы информацию, относящуюся к владельцу пары открытого/секретного ключей, с открытым ключом. Поэтом важно, чтобы процессу управления, в рамках которого формируются эти сертификаты, можно было доверять.

Соглашения с внешними поставщиками криптографических услуг (например, с удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса.

7.8.4. Безопасность системных файлов

Чтобы свести к минимуму риск повреждения ИС, в учреждении необходимо обеспечить контроль над внедрением ПО в рабочих системах.

Тестовые данные должны находиться под контролем и защитой. Для испытаний обычно требуются значительные объёмы тестовых данных, максимально близко соответствующие рабочим данным. Необходимо избегать использования рабочих баз данных, содержащих конфиденциальную информацию. Если эти базы всё же будут использоваться, то конфиденциальные данные должны быть удалены или изменены.

7.8.5. Безопасность процесса разработки и обслуживания систем

Чтобы свести к минимуму вероятность повреждения ИС Общества, следует ввести строгий контроль над внесением изменений. Необходимо установить официальные правила внесения изменений. Эти правила должны гарантировать, что процедуры, связанные с безопасностью и контролем, не будут нарушены, что программисты, занимающиеся поддержкой, получат доступ только к тем частям системы, которые необходимы для их работы, и что для выполнения любого изменения требуется получить официальное разрешение и подтверждение.

После внесения изменений в ИС критичные для бизнес-процессов Общества приложения должны анализироваться и тестироваться, чтобы гарантировать отсутствие вредных последствий для безопасности Общества.

Следует препятствовать внесению изменений в пакеты ПО, за исключением необходимых изменений. Все изменения должны строго контролироваться.

7.9. Управление инцидентами информационной безопасности

В случае возникновении инцидентов сотрудники обязаны обратиться к генеральному директору, и он оценивает типы инцидентов, их масштаб и связанные с ними затраты.

7.10. Аудит информационной безопасности

Общество должно проводить внутренние проверки СУИБ через запланированные интервалы времени.

Основные цели проведения таких проверок:

- оценка текущего уровня защищённости ИС;
- выявление и локализация уязвимостей в системе защиты ИС;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ИР;
- оценка соответствия ИС требованиям настоящей Политики;
- выработка рекомендаций по совершенствованию СУИБ за счёт внедрения новых и повышения эффективности существующих мер защиты информации.
- в число задач, решаемых при проведении проверок и аудитов СУИБ, входят:
- сбор и анализ исходных данных об организационной и функциональной структуре ИС, необходимых для оценки состояния ИБ;
- анализ существующей политики безопасности и других организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);
- технико-экономическое обоснование механизмов безопасности;
- проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности ИС;
- разбор инцидентов ИБ и минимизация возможного ущерба от их проявления.

7.11. Предоставление услуг сторонним организациям

7.11.1. Соглашения о предоставлении услуг

В соглашения о предоставлении услуг сторонним организациям должны быть включены требования безопасности, описание, объёмы и характеристики качества предоставляемых услуг.

7.11.2. Анализ предоставления услуг

Услуги, отчёты и записи, предоставляемые сторонним организациям, должны постоянно проверяться и анализироваться. В отношениях со сторонней организацией должны присутствовать следующие процессы:

- контроль объёма и качества услуг, оговоренных в соглашениях;
- предоставление сторонней организации информации об инцидентах ИБ, связанных с предоставляемыми услугами, и совместное изучение этой информации;
- анализ предоставленных сторонними организациями отчётов о предоставленных услугах;
- управление любыми обнаруженными проблемами.

8. Ответственность

Генеральный директор Общества определяет приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей Политики, утверждает списки объектов и сведений, подлежащих защите, а также осуществляет общее руководство обеспечением ИБ Общества.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ Общества также лежит на генеральном директоре.

Сотрудники Общества несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности генеральному директору.

В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной информации, ставшей известной в силу выполнения своих обязанностей.

Руководство Общества регулярно проводит совещания, посвящённые проблемам обеспечения информационной безопасности с целью формирования чётких указаний по этому вопросу, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению ИБ.

Нарушение требований нормативных актов общества по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.

9. Контроль и пересмотр

Общий и текущий контроль состояния ИБ Общества осуществляется генеральным директором.

Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов ИБ Общества, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

Генеральный директор ежегодно пересматривает положения настоящей политики.

Содержание