ООО «Техно-Телеком»

Приложение
к приказу ООО «Техно-Телеком»
от 02.10.2024 № 33

Политика информационной безопасности
ООО «Техно-Телеком»

2024

Оглавление

1. Общие положения

1.1. Политика информационной безопасности (далее – Политика) определяет основные цели, задачи и принципы обеспечения информационной безопасности, которыми руководствуется ООО «Техно-Телеком» (далее – Общество) в своей деятельности, определяет основные требования по обеспечению информационной безопасности, а также ответственность работников.

1.2. Деятельность по обеспечению информационной безопасности инициирована и контролируется руководителем Общества.

1.3. Соблюдение требований настоящей Политики обязательно для всех работников Общества.

1.4. В настоящей Политике используются следующие термины и определения:

Информация – сведения (сообщения, данные) независимо от формы их представления.

Безопасность информации – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при её обработке.

Конфиденциальность информации – состояние защищенности информации, при котором обеспечивается сохранение информации в тайне от субъектов, не имеющих полномочий на ознакомление с ней.

Целостность информации – состояние защищенности информации, при котором обеспечивается сохранность и неизменность информации при попытках несанкционированных или случайных воздействий на неё в процессе обработки.

Доступность информации – состояние информации, при котором обеспечивается беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Обработка информации – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение,

использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение.

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

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

Уязвимость – недостаток (слабость) программного (программно-технического) средства или ИС в целом, который может быть использован для реализации угроз безопасности информации.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Несанкционированный доступ – доступ к информации или действия с информацией с нарушением правил разграничения доступа.

Локально-вычислительная сеть (ЛВС) – комплекс оборудования и программного обеспечения, обеспечивающий передачу, хранение и обработку информации.

Автоматизированное рабочее место (АРМ) – комплекс средств вычислительной техники и программного обеспечения, предназначенный для выполнения определенных задач, приобретено на средства Общества и состоящий на бухгалтерском учете.

Полный перечень терминов, используемых в настоящей Политике и рекомендуемых к использованию в нормативных и организационно-распорядительных документах, созданных на ее основе, приведен в Приложении № 1 «Термины и определения».

2. Область применения

2.1. В Обществе обрабатывается общедоступная информация, доступ к которой не ограничен, и информация ограниченного доступа, в том числе коммерческая тайна и персональные данные.

2.2. Защите в соответствии с положениями настоящей политики подлежит любая информация, информационные ресурсы и системы Общества, в том числе процессы обработки информации, информационная инфраструктура, включающая помещения, каналы связи, сетевое оборудование, серверы, системы хранения данных, программное обеспечение, средства защиты информации, автоматизированные рабочие места и др.

2.3. Положения настоящей политики не распространяются на сведения, составляющие государственную тайну.

3. Цели обеспечения информационной безопасности

Основными целями обеспечения информационной безопасности, на достижение которых направлены все положения настоящей Политики, являются:

3.1. предотвращение утечки (неконтролируемого распространения) защищаемой информации;

3.2. предотвращение несанкционированного доступа к информации, её уничтожения, модифицирования, блокирования, копирования, иных неправомерных действий;

3.3. предотвращение и (или) снижение возможного материального, физического, морального или иного ущерба от реализации угроз безопасности в процессе обработки информации;

3.4. обеспечение условий быстрого, полного и всестороннего расследования инцидентов информационной безопасности;

3.5. устранение условий возникновения инцидентов информационной безопасности и негативных последствий, в случае их возникновения.

4. Задачи обеспечения информационной безопасности

Для достижения указанных целей необходимо обеспечить эффективное решение следующих задач:

4.1. соблюдение требований законодательства и нормативных документов по защите информации;

4.2. учет всех подлежащих защите информационных ресурсов и систем (каналов связи, сетевого оборудования, серверов, систем хранения данных, программного обеспечения, средств защиты информации, автоматизированных рабочих мест, информационных систем и др.);

4.3. разграничение доступа работников к информации, информационным ресурсам и системам Общества, протоколирование их действий и периодический контроль корректности;

4.4. своевременное выявление угроз безопасности;

4.5. выбор достаточного уровня защиты, при котором затраты, риск и размер возможного ущерба будут приемлемыми для Общества;

4.6. подготовка предложений и реализация мероприятий по информационной безопасности;

4.7. обеспечение необходимого уровня конфиденциальности, целостности и доступности информации при её обработке;

4.8. контроль соблюдения требований по информационной безопасности;

4.9. анализ эффективности принятых мер и их совершенствование.

5. Принципы обеспечения информационной безопасности

При построении и обеспечении функционирования системы информационной безопасности Общество руководствуется следующими принципами:

5.1. Законность

Общество реализует меры по обеспечению информационной безопасности в соответствии с действующим законодательством и договорными обязательствами.

5.2. Системность

Необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов.

5.3. Комплексность

При построении системы защиты используется комплекс методов и средств защиты, которые должны функционировать как целостная система защиты организационно и технически дополняя друг друга.

5.4. Своевременность

Предполагает упреждающий характер мер по обеспечению информационной безопасности, то есть своевременное выявление угроз безопасности с неприемлемыми негативными последствиями (ущербом) и их нейтрализация.

5.5. Разумная достаточность

Меры по обеспечению информационной безопасности выбираются с учетом затрат на их реализацию, вероятности реализации угроз безопасности и размера возможного ущерба.

5.6. Непрерывность

Принятые в Обществе организационные меры по обеспечению информационной безопасности должны непрерывно соблюдаться, перерывы в работе программных и программно-аппаратных средств защиты не должны допускаться.

5.7. Преемственность и совершенствование

Обеспечение информационной безопасности – непрерывный процесс, предполагает постоянное совершенствование методов и средств защиты информации на основе анализа эффективности принятых мер, с учетом изменений информационной инфраструктуры, появления новых угроз безопасности, изменений в методах и средствах перехвата информации, изменений нормативных требований по защите информации.

5.8. Открытость алгоритмов и механизмов защиты

Защита не должна обеспечиваться только за счет конфиденциальности алгоритмов функционирования её подсистем. Знание алгоритмов работы системы защиты не должно давать возможности её преодоления.

5.9. Документированность требований

Все требования по обеспечению информационной безопасности должны быть задокументированы во внутренних документах Общества и утверждены руководителем Общества.

5.10. Осведомленность

Работники Общества должны быть ознакомлены с требованиями по обеспечению информационной безопасности.

5.11. Подбор персонала

Общество стремится тщательно подбирать персонал (работников), формировать и поддерживать корпоративную этику, что создает благоприятную среду для деятельности Общества и снижает риски информационной безопасности.

5.12. Исключение конфликта интересов

Должностные обязанности должны распределяться таким образом, чтобы не возникало ситуаций, при которых личная заинтересованность работника могла бы повлиять на надлежащее, объективное и беспристрастное исполнение им должностных обязанностей и нанести ущерб интересам Общества.

5.13. Минимизация полномочий

Работникам Общества предоставляются минимальные полномочия, необходимые для выполнения возложенных задач. Доступ к информации, информационным ресурсам и системам Общества предоставляется только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

5.14. Персональная ответственность

Работники Общества несут персональную ответственность за нарушение требований по информационной безопасности в пределах своих полномочий. Обязанности соблюдения требований по информационной безопасности включаются в трудовые договоры и должностные инструкции работников.

5.15. Повышение квалификации

Общество повышает квалификацию работников с периодичностью, позволяющей в условиях нарастания количества угроз безопасности, а также с учетом необходимости постоянного совершенствования методов и средств их нейтрализации получать новые знания, умения и навыки, необходимые для профессиональной деятельности.

5.16. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных требований по обеспечению информационной безопасности. Выявленные нарушения доводятся до сведения

руководителей соответствующего уровня и должны оперативно устраняться. Информация о состоянии системы информационной безопасности, существенные недостатки и нарушения установленных требований докладываются руководителю Общества.

6. Требования по обеспечению информационной безопасности

6.1. Подготовка персонала

6.1.1. При приеме на работу руководители подразделений обеспечивают ознакомление работников с внутренними документами Общества по информационной безопасности, с положениями, регламентами, инструкциями, непосредственно связанными с их трудовой деятельностью, под роспись в журналах ознакомления.

6.1.2. Электронные версии документов по информационной безопасности располагаются на файл-сервере ЛВС Общества по адресу «K:\ Texno-telecom\Документы Техно-Телеком\Внутренние документы Общества\ Документы по ИБ».

6.1.3. При утверждении (изменении) внутренних документов Общества руководители подразделений обеспечивают ознакомление работников с документами (изменениями) под роспись в журналах ознакомления.

6.1.4. Работники Общества должны знать и соблюдать требования документов по информационной безопасности, положения, регламенты, инструкции, непосредственно связанные с их трудовой деятельностью.

6.1.5. По распоряжению руководителя Общества может быть создана комиссия и проведена проверка знаний работников по информационной безопасности, положений, регламентов, инструкций, непосредственно связанных с их трудовой деятельностью.

6.1.6. При необходимости, работники Общества могут направляться на курсы повышения квалификации.

6.2. Организация пропускного и внутриобъектового режима

6.2.1. С целью исключения возможности несанкционированного нахождения посторонних лиц на территории Общества, обеспечения безопасности персонала, посетителей, материальных ценностей и информации, в Обществе действует пропускной и внутриобъектовый режим.

6.2.2. В соответствии с Положением по организации пропускного и внутриобъектового режима организована охрана помещений Общества, организованы контрольно-пропускные пункты, оформляются постоянные, разовые и материальные пропуска.

6.2.3. Работникам для прохода на территорию и в помещения Общества оформляются и выдаются постоянные пропуска (электронные пластиковые карты), на основании заявки на выдачу карты и приказа о приеме на работу. При увольнении работника карта изымается.

6.2.4. Доступ в помещение предоставляется работнику только в том случае, если это необходимо для выполнения его должностных обязанностей.

6.2.5. Работники Общества несут персональную ответственность за сохранность выданной им карты. Запрещается передавать карту третьим лицам, в том числе другим работникам Общества.

6.2.6. Работники Общества, получившие карту, обязаны прикладывать её к считывателю при каждом проходе через двери.

6.2.7. Учет, выдача и текущий контроль использования карт работниками Общества осуществляется работниками отдела безопасности и режима.

6.2.8. Проход на охраняемую территорию Общества разрешается:

- работникам, при предъявлении постоянного пропуска (карты), либо по заранее оформленному списку, при предъявлении документа, удостоверяющего личность;

- посетителям, по заранее оформленному списку, при предъявлении разового пропуска и документа, удостоверяющего личность, с записью в книгу учета посетителей.

6.2.9. Посетители и персонал сторонних организаций могут находиться в помещениях Общества только в сопровождении принимающего работника.

6.2.10. Работникам Общества запрещается оставлять незапертыми двери служебных помещений и оставлять ключи в дверных замках в случае временного отсутствия в помещениях работников Общества.

6.2.11. По окончании рабочего дня служебные помещения подлежат обязательной сдаче под охрану работниками оперативному дежурному.

6.2.12. Работники Общества должны соблюдать требования Положения по организации пропускного и внутриобъектового режима.

6.3. Порядок предоставления доступа к информации, информационным ресурсам и системам

6.3.1. Предоставление, изменение, блокирование, прекращение доступа к информации, информационным ресурсам и системам Общества осуществляется работниками отдела безопасности и режима в соответствии с Положением о порядке предоставления доступа к информационным ресурсам.

6.3.2. Доступ к информации, информационным ресурсам и системам Общества предоставляется работнику только в том случае, если это необходимо для выполнения его должностных обязанностей.

6.3.3. Работникам Общества предоставляются минимальные полномочия (чтение, изменение, запись, удаление, выполнение, печать, и др.), необходимые для выполнения возложенных задач.

6.3.4. Доступ предоставляется (изменяется) на основании документально оформленных заявок, согласованных с владельцами информации, информационных ресурсов и систем, либо на основании приказа Общества.

6.3.5. На основании приказа о приеме на работу работникам предоставляется ограниченный доступ к АРМ и ЛВС Общества, корпоративной электронной почте, сети Интернет, общим сетевым ресурсам Общества, общим сетевым ресурсам подразделения, личной сетевой папке.

6.3.6. Для работы с информацией, информационными ресурсами и системами Общества в пределах предоставленных полномочий работник должен ввести свое имя пользователя и индивидуальный пароль.

6.3.7. Руководители подразделений обязаны периодически (не реже одного раза в год) пересматривать необходимые работникам права доступа к информации, информационным ресурсам и системам Общества и их минимальные полномочия.

6.3.8. Прекращение или блокирование доступа к информации, информационным ресурсам и системам Общества осуществляется на основании документально оформленных заявок, либо на основании приказа Общества (приказа о предоставлении отпуска по уходу за ребенком, приказа об увольнении (переводе) работника).

6.3.9. В случае необходимости предоставления доступа к информационным ресурсам и системам Общества персоналу сторонних организаций для настройки, обновления, консультирования и других действий, руководитель

подразделения обязан заранее уведомить начальника отдела безопасности и режима.

6.3.10. Заявки на предоставление, изменение, блокирование и прекращение доступа хранятся в отделе безопасности и режима.

6.3.11. Работники Общества должны соблюдать требования Положения о порядке предоставления доступа к информационным ресурсам.

6.4. Организация парольной защиты

6.4.1. Организационно-техническое обеспечение процессов создания, изменения, блокирования, удаления учетных записей и процессов генерации, использования, изменения и прекращения действия паролей в ЛВС Общества осуществляется работниками отдела безопасности и режима в соответствии с Положением по организации парольной защиты.

6.4.2. Защите паролем подлежит доступ к информации, информационным ресурсам и системам Общества, в том числе доступ к настройкам операционных систем, средств антивирусной защиты, средств защиты информации, сетевого и серверного оборудования, BIOS АРМ, многофункциональных устройств и др.

6.4.3. Имя пользователя и индивидуальный пароль (учетная запись) являются идентификатором работника Общества.

6.4.4. Работник Общества обязан запомнить своё имя пользователя и индивидуальный пароль.

6.4.5. При вводе пароля необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами.

6.4.6. Работникам Общества **запрещается**:

- записывать пароли на бумаге, в файлах, электронной записной книжке, мобильном телефоне, на любых других предметах и носителях информации;

- сообщать кому-либо свой пароль полностью или частично;

- спрашивать или подсматривать пароль других работников;

- предоставлять доступ третьим лицам к информации, информационным ресурсам и системам Общества под своей учетной записью;

- авторизоваться в ЛВС Общества под учетной записью другого работника.

6.4.7. В случае компрометации личного пароля, работник Общества должен немедленно принять меры по внеплановому изменению пароля и письменно доложить о факте компрометации администратору ЛВС, непосредственному руководителю и начальнику отдела безопасности и режима.

6.4.8. При временном оставлении рабочего места в течение рабочего дня, работник Общества обязан заблокировать АРМ нажатием комбинации клавиш «Win + L», либо «Ctrl + Alt + Delete» и выбрать действие «Заблокировать».

6.4.9. Работники Общества несут персональную ответственность за все действия, совершенные от имени их учетной записи, если с их стороны не были выполнены требования для предотвращения её компрометации.

6.4.10. Работники Общества должны соблюдать требования Положения по организации парольной защиты.

6.5. Организация антивирусной защиты

6.5.1. Для защиты информации, информационных ресурсов и систем Общества от вредоносных программ, их обнаружения, блокирования, изолирования и удаления используются средства антивирусной защиты.

6.5.2. Приобретение, установка, настройка, обновление и контроль использования средств антивирусной защиты в Обществе осуществляется работниками отдела безопасности и режима в соответствии с Положением по организации антивирусной защиты.

6.5.3. В Обществе разрешается использование лицензионных, централизовано приобретенных, управляемых средств антивирусной защиты.

6.5.4. Работникам Общества запрещается использование АРМ без работающего средства антивирусной защиты. Работники обязаны убедиться в успешности загрузки средства антивирусной защиты, подтверждением загрузки является наличие в правом нижнем углу на панели задач иконки используемого средства антивирусной защиты.

6.5.5. Работники Общества сразу после подключения носителей информации (флеш-карты, SD-карты, жесткие и твердотельные диски, оптические диски, мобильные устройства и др.) к АРМ обязаны проверить их средствами антивирусной защиты.

6.5.6. В случае обнаружения на носителях информации вредоносных программ, использование носителей информации разрешается только после удаления вредоносных программ.

6.5.7. Работники Общества обязаны проверять средствами антивирусной защиты любую информацию (файлы любых форматов) получаемую/ передаваемую по каналам связи, через облачные сервисы, электронную почту.

6.5.8. Проверку входящей информации необходимо проводить непосредственно после её приема, проверку исходящей информации необходимо проводить непосредственно перед её передачей.

6.5.9. Запрещается открывать файлы и ссылки, запускать программы, полученные от неизвестного отправителя, либо подозрительного содержания.

6.5.10. При возникновении подозрения на наличие вредоносных программ на АРМ (ошибки при загрузке операционной системы, медленная работа, частые зависания и сбои АРМ, нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, исчезновение файлов и папок и т.п.) работник Общества должен отключить АРМ от ЛВС Общества, запустить полную проверку АРМ средствами антивирусной защиты, уведомить работников отдела безопасности и режима.

6.5.11. Работники Общества должны выполнять мероприятия в соответствии с Положением по организации антивирусной защиты.

6.6. Организация резервного копирования и восстановления

6.6.1. Резервное копирование, архивирование и восстановление информации, информационных ресурсов и систем Общества осуществляется в соответствии с Положением по резервному копированию и восстановлению информации.

6.6.2. Резервное копирование выполняется с целью обеспечения возможности восстановления информации, информационных ресурсов и систем Общества в случае сбоя или выхода из строя оборудования, программного обеспечения, воздействия вредоносных программ, случайного или преднамеренного уничтожения информации, чрезвычайных обстоятельств.

6.6.3. Резервное копирование информации, информационных ресурсов и систем на серверах ЛВС Общества выполняют работники отдела безопасности и режима.

6.6.3.1. Резервное копирование осуществляется с использованием специализированного программного обеспечения.

6.6.3.2. Задачи резервного копирования настраиваются в соответствии с планом резервного копирования (наименование ресурса, расположение ресурса, вид копирования, расписание копирования, расположение копии).

6.6.3.3. Хранение резервных копий осуществляется на сетевых хранилищах.

6.6.3.4. Контроль результатов резервного копирования осуществляют работники отдела безопасности и режима ежедневно.

6.6.4. Резервное копирование информации на АРМ выполняют работники Общества.

6.6.4.1. Состав информации, периодичность резервного копирования, срок хранения резервных копий, определяется исходя из необходимости обеспечения непрерывности бизнес-процессов Общества в случае повреждения или утраты информации на АРМ.

6.6.4.2. Хранение резервных копий осуществляется на дополнительном физическом диске АРМ (при наличии) и в личной сетевой папке, на общем сетевом ресурсе подразделения, разрешенных к использованию в Обществе носителях информации, оптических дисках.

6.6.4.3. Работники отдела безопасности и режима оказывают содействие работникам Общества в выполнении резервного копирования на соответствующие носители.

6.6.5. Запрещается хранение резервных копий в облачных сервисах сети Интернет без заключения соглашения об обеспечении конфиденциальности информации.

6.6.6. В случае сбоев, отказов технических средств и программного обеспечения осуществляется обязательное восстановление информации, информационных ресурсов и систем Общества.

6.6.7. Работники Общества должны выполнять мероприятия в соответствии с Положением по резервному копированию и восстановлению информации.

6.7. Использование оборудования

6.7.1. Приобретение, установка, настройка, техническая поддержка и модернизация оборудования информационной инфраструктуры Общества

(системные блоки, ноутбуки, мониторы, принтеры, сканеры, многофункциональные устройства, источники бесперебойного питания, сетевое оборудование, серверы, системы хранения данных и др.) осуществляется (организуется) работниками отдела безопасности и режима.

6.7.2. Необходимое оборудование приобретается на средства Общества, принимается к бухгалтерскому учету и передается руководителю подразделения для использования в производственных и служебных целях.

6.7.3. Конфигурация АРМ должна соответствовать должностным обязанностям работника Общества.

6.7.4. Неиспользуемые для исполнения должностных обязанностей устройства, адаптеры, порты ввода-вывода на АРМ (COM, LPT, USB, IR, NFC, Wi-Fi, Bluetooth, оптические приводы, др.) отключаются.

6.7.5. Работникам Общества запрещается самостоятельно разбирать, вносить изменения в конструкцию, конфигурацию, подключение и размещение АРМ.

6.7.6. Работник Общества обязан бережно относиться к используемому оборудованию, принимать все необходимые меры для обеспечения его сохранности, не допускать попадания влаги на поверхность оборудования, использовать оборудование исключительно для выполнения своих должностных обязанностей, выключать оборудование в конце рабочего дня.

6.7.7. Работники Общества, использующие в работе ноутбуки, смартфоны, планшеты, носители информации и др., обязаны принимать надлежащие меры по обеспечению их сохранности, как в офисе, так и в иных местах (в автомобилях, конференц-залах, гостиницах, аэропортах и т.д.), обязаны ни при каких обстоятельствах не оставлять их без присмотра. В случае утери (кражи) указанных устройств ответственность возлагается на работника.

6.7.8. Работникам Общества запрещается приносить и использовать в работе личные устройства и оборудование без письменного разрешения руководителя Общества. Оформленные и согласованные руководителем Общества разрешения направляются в отдел безопасности и режима.

6.7.9. Вышедшее из строя, морально устаревшее, не используемое в течение календарного года оборудование подлежит списанию и утилизации. Перед утилизацией носители информации демонтируются и уничтожаются, либо выполняется процедура удаления данных без возможности восстановления.

6.7.10. Работники Общества при эксплуатации оборудования должны соблюдать указанные требования.

7. Ответственность

7.1. Работники Общества, нарушившие требования настоящей Политики могут быть привлечены к ответственности в соответствии с действующим законодательством и локальными нормативными актами Общества.

7.2. Форма и степень ответственности определяется исходя из вида и размера ущерба, нанесенного Обществу действиями либо бездействием соответствующего работника.

7.3. Отдел безопасности и режима контролирует исполнение работниками Общества положений настоящей Политики.

7.4. Информация, запротоколированная в журналах событий, может служить доказательством нарушений работниками Общества требований настоящей Политики.

7.5. О выявленных нарушениях настоящей Политики начальник отдела безопасности и режима докладывает генеральному директору Общества и заместителю генерального директора Общества по безопасности.

7.6. Работники Общества должны быть ознакомлены с настоящей Политикой под роспись в журнале ознакомления.

8. Нормативные ссылки

При разработке настоящей Политики учтены требования и рекомендации следующих документов:

- ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности»;
- ИСО/МЭК 27005 «Информационные технологии. Методы обеспечения безопасности. Выбор мер обеспечения информационной безопасности»;
- «Методический документ. Методика оценки угроз безопасности информации», утвержден ФСТЭК России 5 февраля 2021 г.
- ГОСТ Р ИСО/МЭК то 18044-2007. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.»

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
- Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»
- Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»
- Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»
- Постановление Правительства РФ от 13 февраля 2019 г. № 127 «Об утверждении требований к обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и уровней обеспеченности безопасности»
- Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»
- Федеральный закон от 8 февраля 1998 г. № 14-ФЗ «Об организации с ограниченной ответственностью»
- Постановление Правительства РФ от 31 октября 2018 г. № 1277 «Об утверждении правил аккредитации организаций, осуществляющих деятельность в области информационной безопасности»
- Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Положения об организации и осуществлении государственного контроля в области защиты государственной тайны»
- Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении требований к средствам криптографической защиты информации»
- Доктрина информационной безопасности Российской Федерации

9. Структура и ответственность

В этом разделе представлены основные положения политики информационной безопасности Общества. Более детальная информация содержится в соответствующих разделах и положениях.

9.1. Структура политики ИБ:

Политика ИБ ООО “Техно-Телеком” включает следующие ключевые элементы:

9.1.1. Цели и задачи ИБ:

Обеспечение целостности, доступности и конфиденциальности информационных активов компании.

9.1.2. Принципы ИБ:

Соответствие законодательным и нормативным требованиям, непрерывность защиты, ответственность всех сотрудников за соблюдение политики ИБ.

9.1.3. Меры и средства обеспечения ИБ:

Использование современных технических решений (антивирусы, фаерволы, шифрование данных), регулярное обновление программного обеспечения и оборудования.

9.1.4. Процессы управления ИБ:

Планирование мероприятий по ИБ, реализация защитных мер, мониторинг состояния безопасности, проведение аудитов и корректировка мер при необходимости.

9.1.5. Ответственность и полномочия:

Распределение обязанностей между отделом ИТ, службой безопасности и руководством компании.

9.2. Ответственность за соблюдение политики ИБ

9.2.1. Отдел ИТ:

Внедрение и поддержка технических мер защиты, обучение сотрудников правилам безопасного использования информационных систем.

9.2.2. Служба безопасности:

Проведение регулярных проверок безопасности, реагирование на инциденты ИБ, взаимодействие с правоохранительными органами при необходимости.

9.2.3. Руководство компании:

Утверждение бюджета на ИБ, контроль за выполнением политики ИБ, принятие решений о внесении изменений в политику.

9.3. Полномочия и обязанности

9.3.1. Отдел ИТ:

Установка и настройка средств защиты, обновление антивирусных баз, мониторинг событий безопасности.

9.3.2. Служба безопасности:

Проведение расследований инцидентов ИБ, разработка рекомендаций по улучшению защиты, участие в аудите безопасности.

9.3.3. Руководство компании:

Принятие решений о закупке новых средств защиты, утверждение изменений в политике ИБ, контроль за соблюдением законодательства в области ИБ.

9.4. Контроль и отчётность

9.4.1. Регулярные проверки:

Проведение внутренних и внешних аудитов безопасности, оценка эффективности мер защиты.

9.4.2. Отчётность:

Предоставление руководству отчётов о состоянии ИБ, информирование сотрудников о выявленных уязвимостях и мерах по их устранению.

10. Осведомленность и информирование

10.1. Порядок и способы обеспечения осведомленности и информирования сотрудников в области информационной безопасности:

- Проведение обучающих семинаров и вебинаров, направленных на повышение осведомленности сотрудников о текущих угрозах информационной безопасности и методах защиты данных.
- Проведение регулярных рассылок информационных бюллетеней, содержащих актуальные новости, рекомендации и лучшие практики в области информационной безопасности.
- Обеспечение актуальности и доступности информации о новых угрозах и изменениях в политике безопасности, вовлекая сотрудников в обсуждение данных вопросов.

10.2. Ответственность за выполнение осведомленности и информирования работников организации возлагается на руководство Организации и руководителей структурных подразделений

11. Контроль

11.1. Объекты контроля

Контролю подлежат все информационные системы, включая программное обеспечение, операционные системы и сетевые устройства. Также контролируются базы данных, хранящие информацию, и документы, содержащие персональные данные, чувствительные для Общества. Учитываются все физические носители информации.

11.2. Формы контроля

Контроль осуществляется в форме регулярных аудитов, которые включают всестороннюю оценку.

11.3. Периодичность

Мониторинг осуществляется систем безопасности с использованием специализированного программного обеспечения, анализ инцидентов безопасности с целью выявления причин и предотвращения повторения, а также проверки соблюдения установленных политик и процедур информационной безопасности путём проведения регулярных инспекций.

Аудиты информационной безопасности проводятся не реже одного раза в год, чтобы своевременно выявлять недостатки и риски. Мониторинг систем осуществляется ежемесячно для обеспечения постоянного контроля за состоянием ресурсов Общества. Анализ инцидентов проводится по мере их возникновения.

Совершенствование системы управления информационной безопасностью (СУИБ) Организации осуществляется с целью поддержания актуальности и эффективности мер защиты информации, адаптации к изменяющимся условиям внешней и внутренней среды, а также в соответствии с требованиями законодательства и нормативных актов.

12. Порядок совершенствования

12.1. Предпринимаемые действия по совершенствованию СУИБ

Для обеспечения актуальности действующей системы управления информационной безопасности Общества предпринимаются следующие действия:

- регулярный анализ текущих угроз, уязвимостей и рисков, связанных с информационной безопасностью;
- внедрение новых технологий и решений с целью защиты информации, повышение эффективности уже существующих мер;
- проведение внутренних и внешних аудитов информационной безопасности для оценки состояния СУИБ и выявления потенциальных проблем;
- повышение квалификации сотрудников в сфере информационной безопасности.

12.2. Порядок мониторинга ИБ и реагирования на инциденты

Мониторинг информационной безопасности осуществляется непрерывно с помощью автоматизированных систем, отвечающих за:

- контроль сетевой активности и действий пользователей;
- регистрацию и анализ инцидентов безопасности;
- своевременное уведомление ответственных лиц о подозрительных событиях и потенциальных нарушениях безопасности.

Реагирование на инциденты ИБ проводится согласно положению «Реагирование на инциденты информационной безопасности».

12.3. Порядок принятия решений по совершенствованию СУИБ

Решения о совершенствовании СУИБ принимаются на основе:

- результатов внутренних аудитов и анализа инцидентов;
- изменений во нормативно-правовой базе и требованиях законодательства;
- выявленных рисков и угроз, а также предложений по модернизации системы управления информационной безопасности от сотрудников Общества или регуляторов.

Предложения по улучшению СУИБ выносятся на рассмотрение начальников отдела безопасности и режима, согласуются с руководством

Общества и утверждаются директором. Внедрение новых мер и процедур осуществляется после утверждения приказом директора.

12.4. Порядок принятия, пересмотра, отмены организационно-распорядительных документов по ИБ

Принятие, пересмотр и отмена организационно-распорядительных документов по информационной безопасности осуществляется в следующем порядке:

- разработка нового документа инициируется на основе выявленных потребностей в изменении СУИБ или изменения законодательных требований;
- документы разрабатываются начальников отдела безопасности и режима;
- документ утверждается директором Общества на основании представленного проекта и заключения ответственных лиц;
- пересмотр и отмена документов проводится по мере необходимости, но не реже одного раза в год;

Начальник отдела безопасности и режима Б.Б. Бобурченко
ООО «Техно-Телеком»

СОГЛАСОВАНО
Заместитель генерального директора Р.Р. Ромашков
ООО «Техно-Телеком»