Открытое акционерное
общество «Гипросвязь»

УТВЕРЖДАЮ
Директор ОАО «Гипросвязь»
_____ А.Е. Алексеев
"___" _____ 2022 г.

ПОЛИТИКА
ОАО «Гипросвязь»
по обеспечению
информационной безопасности

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящий документ определяет политику открытого акционерного общества «Гипросвязь» (далее – Общество) в отношении обеспечения информационной безопасности, направленной на защиту информации при осуществлении своей деятельности.

1.2 Политика по обеспечению информационной безопасности (далее – Политика) разработана с учетом требований:

Закона Республики Беларусь № 455-З от 10 ноября 2008 года «Об информации, информатизации и защите информации»;

Закона Республики Беларусь N 99-З от 7 мая 2021 года «О защите персональных данных»;

Закона Республики Беларусь от 5 января 2013 г. № 16-З «О коммерческой тайне»;

Указа Президента Республики Беларусь от 16 апреля 2013 года №196 «О некоторых мерах по совершенствованию защиты информации»;

Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575;

Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1;

Положения о порядке технической и криптографической защиты информации в информационных системах (далее – ИС), предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66.

1.3 Политика распространяется на персонал (штатных работников, совместителей) Общества, привлекаемых по гражданско-правовым договорам физических лиц, а также юридических лиц, участвующих в эксплуатации (использующих в своей работе), обслуживании, поддержке объектов информационной системы (далее – ОИС), программного обеспечения (прикладного и системного) (далее – ПО), информационных ресурсов (далее – ИР), ИС Общества (собственных, либо предоставленных в рамках договоров).

1.4 Общее руководство системой информационной безопасности (далее – ИБ), принятие всех решений по вопросам ее функционирования, а также контроль за организацией работы по обеспечению ИБ возлагается на директора Общества. На заместителей директора Общества возлагается ответственность за обеспечение ИБ по направлениям в соответствии с распределением обязанностей.

1.5 Работы по обеспечению ИБ в Обществе выполняет сектор эксплуатации вычислительной техники и локальной сети (далее – СЭВТиЛС) в соответствии с локальными правовыми актами (далее – ЛПА), устанавливающими порядок осуществления деятельности по обеспечению ИБ в организации. В Обществе обеспечивается наличие лиц, обладающих необходимой квалификацией и прошедших соответствующее обучение, а также повышение квалификации не реже 1 раза в 3 года по вопросам ИБ.

1.6 В качестве правовых и организационных мер, направленных на обеспечение защиты информации применяются:

положение о полномочиях работников ОАО «Гипросвязь» при работе в системе корпоративной информационной технологической сети;

отдельные руководящие документы на время их действия;

указания руководителя организации (уполномоченного должностного лица);

обязательства о неразглашении сведений, составляющих коммерческую тайну.

2. ЦЕЛЬ И ПРИНЦИПЫ ПОЛИТИКИ

2.1 Политика Общества по обеспечению ИБ направлена на гармонизацию подходов и требований по обеспечению ИБ для персонала Общества, представителей юридических лиц, индивидуальных предпринимателей, а также физических лиц, работающих на основании заключенных с Обществом гражданско-правовых договоров и имеющих доступ к сети передачи данных ОАО «Гипросвязь», информационным ресурсам и (или) технологиям Общества (далее – субъекты информационных отношений) при осуществлении Обществом своей деятельности.

Требования настоящей Политики не распространяются на сведения, содержащие государственные секреты.

2.2 Основными целями Политики является обеспечение ИБ, а именно:

снижение уровня рисков, связанных с ИБ;

снижение числа инцидентов, связанных с ИБ;

повышение компетентности персонала в области ИБ;

улучшение имиджа Общества и минимизация ущерба вследствие возможного возникновения инцидентов ИБ;

обеспечение непрерывности бизнес-процессов;

обеспечение соответствия требованиям законодательства, стандартам и договорным обязательствам в части ИБ.

2.3 Достижение указанных целей осуществляется посредством выполнения следующих мероприятий:

реализация требований законодательства Республики Беларусь в части ИБ и мер контроля их защищенности;

определение ответственности субъектов информационных отношений (далее – субъектов) по обеспечению и соблюдению требований Политики, в том числе с использованием ИР, ИС и ОИС, а также посредством принятие соответствующих внутренних ЛПА по обеспечению информационной безопасности Общества;

своевременное выявление и оценка причин, условий и характера угроз ИБ, а также дальнейшее прогнозирование развития событий на основе мониторинга инцидентов ИБ;

планирование, реализация и контроль эффективности использования мер и средств защиты информации, создание механизма оперативного реагирования на угрозы ИБ;

повышение осведомленности и обучение персонала Общества возможным факторам рисков ИБ и мерам противодействия им.

2.4 Защита информации в Обществе строится на основе следующих принципов:

законности, согласно которому принимаемые меры должны строго соответствовать действующему законодательству;

упреждения, который предполагает своевременное выявление тенденций и предпосылок, способствующих развитию угроз, и принятие предупреждающих мер;

непрерывности, согласно которому защита информации осуществляется на постоянной основе;

системности, который предусматривает системный и комплексный подход к защите информационных систем и ресурсов Общества;

компетентности и специализации, которые предполагают наличие работников, обладающих необходимой совокупностью знаний, навыков и опыта в сфере защиты информации;

осведомленности, что предполагает доведение информации о требованиях по защите информации до всех работников;

достаточности, который предполагает анализ принимаемых мер по защите информации и выработку оптимальных решений для достижения и поддержания приемлемого уровня безопасности.

3. СУБЪЕКТЫ, ОБЪЕКТЫ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ И ПОРЯДОК ИХ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

3.1 Субъектами являются:

Общество, выступающее в качестве обладателя информации и собственника ИР, ИС и ОИС;

государственные органы и организации, юридические лица, в том числе индивидуальные предприниматели, физические лица эксперты, выступающие в качестве пользователей ИР, ИС и ОИС Общества;

иные юридические лица, в том числе иностранные, международные организации, выступающие в качестве информационных посредников, операторов информационных систем и связи, поставщиков ОИС, а также в качестве поставщика услуг Общества, в том числе технической поддержки и сервисного обслуживания.

3.2 Субъектами в рамках Общества являются внутренние и внешние пользователи:

3.2.1 внутренние пользователи:

- работники СЭВТиЛС, осуществляющие обеспечение безопасного использования ИР, ИС и ОИС;
- персонал Общества, получивший доступ к ИР, ИС и ОИС Общества и использующий их в рамках выполнения своих функциональных обязанностей.

3.2.2 внешние пользователи:

- государственные органы и организации в рамках передачи отчетности и получения электронных сообщений;
- посетители Общества, обратившиеся за оказанием услуг;
- физические лица эксперты;

– должностные лица организаций, поставляющие ИР, ИС и ОИС для Общества и осуществляющие их гарантийное и сервисное обслуживание.

3.3 Ответственность субъектов информационных отношений за обеспечение защиты информации в Обществе установлена в следующих документах:

положении о полномочиях работников ОАО «Гипросвязь» при работе в системе корпоративной информационной технологической сети (для внутренних пользователей);

организационно-распорядительных документах Общества;

должностных инструкциях работников Общества (для внутренних пользователей);

иных документах, в том числе соглашениях и договорных обязательствах при оказании услуг.

3.4 Объектами информационных отношений (далее – объекты) являются:

информация, хранящаяся и обрабатываемая в информационных системах Общества, а также передаваемая при оказании Обществом услуг для сторонних организаций, в том числе конфиденциальная;

информационная инфраструктура, включающая ИР, ИС и ОИС.

3.5 Порядок информационного взаимодействия объектов между собой определяется соответствующей эксплуатационной (технической) документацией по ее использованию.

3.6 Основными составляющими объектами Общества являются компоненты, входящие в состав информационной инфраструктуры организации:

локальная вычислительная сеть;

информационные системы;

отдельные рабочие места, предназначенные для доступа, хранения и обработки информации, распространения и (или) предоставления которой ограничено;

другие технические средства, с установленным системным и прикладным программным обеспечением, и средствами управления базами данных, используемые для сбора, хранения, обработки и передачи информации, в том числе подключаемые съемные носители.

4. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1 Под угрозой применительно к Политике понимается потенциальная возможность случайного или преднамеренного воздействия на объект защиты, вследствие которого причиняется вред целостности, конфиденциальности, доступности и сохранности информации.

4.2 Случайное воздействие на объект защиты предполагает наступление негативных последствий вследствие неумышленных действий либо стечения обстоятельств, таких как стихийные бедствия и аварии, сбои и отказы технических средств, ошибки при разработке информационных систем, алгоритмические и программные ошибки, ошибки пользователей и администраторов сети и т.д.

4.3 Преднамеренное воздействие на объект защиты является результатом умышленных действий, когда наступлению негативных последствий предшествуют неправомерный доступ к информации, ее несанкционированное копирование, изменение либо изъятие, применение запрещенного программного обеспечения и неразрешенных к использованию технических средств, разработка и распространение вирусных программ и пр.

4.4 Характерные признаки реализации угроз проявляются в инцидентах информационной безопасности (далее – инциденты), выражающихся в непредвиденных и нежелательных событиях, способных оказывать негативное влияние на состояние защищенности информации.

5. РАЗГРАНИЧЕНИЕ ДОСТУПА СУБЪЕКТОВ К ОБЪЕКТАМ ОБЩЕСТВА

5.1 Субъекты имеют необходимый уровень доступа к объектам Общества, назначенный в соответствии с принципом минимизации прав, назначаемых пользователям (это означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации и настройкам предоставляется только в том случае и объеме, если это необходимо пользователю для выполнения его должностных обязанностей:

работникам СЭВТиЛС предоставляется доступ к объектам в соответствии с их ответственностью и полномочиями;

персоналу Общества предоставляется доступ к объектам в рамках выполнения ими соответствующих должностных обязанностей;

персоналу, участвующему в процессе оказания услуг заказчикам, предоставляется доступ к информации, содержащейся в ИР и ИС, необходимой для оказания этих услуг в соответствии с документами системы менеджмента качества Общества;

лицам, поставляющим ОИС, а также осуществляющим их гарантийное, сервисное обслуживание и жизнеобеспечение, предоставляется доступ к объектам в рамках договорных отношений на оказание услуг;

в рамках договорных отношений по предоставлению услуг со стороны Общества;

в рамках Заявлений и Соглашений;

в рамках документов системы менеджмента качества;

в случае необходимости посетителям Общества предоставляются исключительно гостевой доступ к сетям, либо устройствам, с ограниченным доступом к ИС и ИР Общества.

5.2 Порядок и правила предоставления доступа к объектам Общества определяются следующими документами:

политикой по обеспечению информационной безопасности;

положением о полномочиях работников ОАО «Гипросвязь» при работе в системе корпоративной информационной технологической сети;

договорными отношениями при оказании Обществом услуг, в том числе технической поддержки;

должностными инструкциями работников Общества;

положением об СЭВТиЛС;

иными ЛПА Общества.

5.3 Делопроизводство по документам, содержащим служебную информацию ограниченного распространения, регулируется положением о порядке ведения делопроизводства по документам, содержащим служебную информацию ограниченного распространения, и порядке обращения со служебной информацией ограниченного распространения в ОАО «Гипросвязь».

5.4 Разграничение доступа к информационным системам и их объектам осуществляется с помощью средств управления правами доступа к соответствующим активам. К указанным средствам относятся:

групповые политики безопасности;

средства управления доступом операционных систем;

средства управления доступом к официальному сайту Общества;
средства управления доступом к хостингам сайта и электронной почты;
средства управления доступом к ИС, ИР, ОИС Общества;
средства управления доступам к электронной почте Общества;
средства управления доступом к базам данных Общества;
средства управления доступом к системам хранения данных Общества;
средства управления доступом к информационным системам и их объектам, информационным ресурсам, предоставленным пользователям в рамках выполнения должностных обязанностей и договорных отношений.

5.5 Разграничение доступа к вышеуказанным активам Общества включает в себя:
регистрацию и идентификацию пользователей;
аутентификацию пользователей;
авторизацию пользователей для получения доступа;
регистрацию и учет попыток доступа к защищаемым активам.

5.6 При определении полномочий каждого авторизованного пользователя выполняются следующие условия:
полномочия пользователя соответствуют его должностным обязанностям и осуществляются только в границах этих полномочий;
полномочия пользователя должны распространяться на конкретные категории информации, информационных систем и их объектов, информационных ресурсов.

5.7 С целью разграничения прав доступа работников к объектам Общества используются роли безопасности. В базовом варианте Обществом применяются следующие роли безопасности: роль «Администратор» и «Пользователь». В случае необходимости более детального разграничения применяются дополнительные роли, в зависимости от конкретной ИС и ИР.

5.8 Назначение ролей пользователей информационной инфраструктуры Общества осуществляется исходя из выполняемых ими функциональных обязанностей. Для каждой роли в отношении единицы актива определен и\или ограничен список допустимых операций. Допускается совмещение нескольких ролей одним работником по функциям, не оказывающим влияния на уровень безопасности объекта в том случае если эти роли не являются взаимоисключающими.

Каждой роли соответствуют определенные права доступа субъекта к объекту – авторизованный пользователь. Ролевое деление авторизованных пользователей реализуется с помощью функциональных возможностей разграничения доступа к информационным системам и их объектам, информационным ресурсам.

В случае предоставления пользователю новой роли его права доступа к защищаемым данным и информационной инфраструктуре Общества пересматриваются.

В случае увольнения или перевода работника Общества в другое структурное подразделение либо на другую должность его права доступа пересматриваются, а в необходимых случаях – блокируются.

В случае выявления инцидентов безопасности права доступа авторизированного пользователя блокируются (либо ограничиваются) до завершения рассмотрения инцидента.

5.9 ОИС (за исключением ПК и мобильных устройств, используемых в служебных целях вне территории Общества) располагаются в помещениях, исключающих несанкционированный доступ к ним и обеспечивающих их бесперебойную круглосуточную эксплуатацию в климатических условиях, указанных в документации на эксплуатацию.

6. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

6.1 Субъекты информационных отношений в пределах предоставленных им полномочий и (или) прав при использовании объектов информационных отношений имеют право:

использовать ОИС для доступа к ИС и ИР, другим ОИС с целями поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления и пользования информацией;

осуществлять иные действия в соответствии с должностными инструкциями и ЛПА Общества.

6.2 Субъекты информационных отношений в пределах предоставленных им полномочий и (или) прав при использовании объектов информационных отношений обязаны:

соблюдать права других лиц при использовании объектов Общества;

исполнять обязанности в соответствии с должностными инструкциями и локальными правовыми актами Общества.

6.3 Права и обязанности субъектов Общества регламентированы следующими документами:

положением о полномочиях работников ОАО «Гипросвязь» при работе в системе корпоративной информационной технологической сети;

должностными инструкциями работников Общества.

6.4 Общество обязуется постоянно совершенствовать систему информационной безопасности, обеспечивать ресурсами, достаточными для достижения указанных в настоящей политике целей, а также соответствовать всем обязательным и\или применимым законодательным, нормативным, договорным и иным требованиям.

7. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ОБЪЕКТОВ ОБЩЕСТВА С ИНЫМИ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ И СИСТЕМАМИ

7.1 Порядок взаимодействия объектов Общества с иными информационными системами определяется соответствующими документами по каждому взаимодействию.

7.2 Функционирование объектов Общества осуществляется с обновлением системного, прикладного программного обеспечения и антивирусных баз с соответствующих ресурсов.

7.3 Обновление баз средств защиты информации от действий вредоносного ПО и файлов осуществляется с периодичностью, установленной производителем антивирусного программного обеспечения.

7.4 Доступ к сети Интернет предоставляется только авторизованным сервисам и пользователям.

7.5 К авторизованным сервисам Общества относятся:

обновление системного и прикладного ПО;

обновление встроенного ПО технических средств;

обновление баз средств защиты информации от действий вредоносного ПО и файлов;

синхронизация времени с надежным источником времени.

7.6 Правила доступа к сетям общего пользования определены и регулируются положением о полномочиях работников ОАО «Гипросвязь» при работе в системе корпоративной информационной технологической сети.

7.7 При взаимодействии объектов Общества с иными ИС применяются средства защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы.

7.8. Взаимодействие с ИС сторонних организаций используется в целях обмена информацией, необходимой для реализации возложенных на Общество функций.

7.9. При взаимодействии со сторонними ИС по открытым каналам передачи данных применяются следующие меры обеспечения защиты активов от угроз со стороны внешних подключений:

фильтрация сетевых пакетов в соответствии с задаваемыми правилами на основе IP-адресов отправителя и получателя, разрешенных портов, протоколов и приложений;

управление сетевым доступом к сегментам СПД;

трансляция сетевых адресов для сокрытия топологии сети;

обнаружение и предотвращение атак с использованием известных шаблонов атак;

защита от атак типа «отказ в обслуживании»;

обновление базы сигнатур подсистемы обнаружения и предотвращения вторжений;

антивирусная фильтрация трафика, получаемого из сети Интернет;

использование защищённых каналов передачи данных со сторонними информационными системами;

регистрация событий информационной безопасности с заданным уровнем детализации.

7.10 При обмене файлами по открытым каналам передачи данных необходимо использовать протоколы со встроенными механизмами шифрования (в частности, SFTP). Для передачи общедоступной информации допускается использовать протоколы без встроенных механизмов шифрования.

8. ПОРЯДОК ПЕРЕСМОТРА ПОЛИТИКИ

По мере совершенствования законодательства, развития систем автоматизации, внедрения новых услуг Политика может пересматриваться или дополняться.

Актуализация Политики проводится при необходимости, но не реже одного раза в три года с целью приведения в соответствие защитных мер современным угрозам и актуализации требований по защите информации. Внеплановая корректировка Политики проводится в обязательном порядке в следующих случаях:

при изменении нормативных правовых актов и (или) документов Общества, касающихся информационной безопасности информационных систем и информационных ресурсов;

при возникновении в процессе деятельности по защите информации ситуаций и (или) инцидентов, которые создают угрозу безопасного функционирования информационных ресурсов, но необходимость реагирования на них не предусмотрена Политикой.

Положения настоящей Политики могут дополняться и уточняться другими внутренними техническими документами Общества.