ОСК.КСМК 00.011-2023

Приложение

УТВЕРЖДЕНА
приказом АО «ОСК»
от «20» 12 2023 г. № 406

КОНЦЕПЦИЯ

информационной безопасности АО «ОСК» и обществ Группы ОСК

Санкт-Петербург
2023

Оглавление

I. Список сокращений

АО «ОСК» – акционерное общество «Объединенная судостроительная корпорация»;

АС – автоматизированная система;

ГосСОПКА – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

ЗИ – защита информации;

ИБ – информационная безопасность;

ИС – информационная система;

ИТР – иностранная техническая разведка;

кибератака – целевая компьютерная атака;

КИИ – критическая информационная инфраструктура;

НКЦКИ – Национальный координационный центр по компьютерным инцидентам;

НСД – несанкционированный доступ;

образец ВВТ – образец вооружения и военной техники;

ПД ИТР – противодействие иностранным техническим разведкам;

ПДн – персональные данные;

ПО – программное обеспечение;

САПР – система автоматизации проектных работ;

СЗИ – средство защиты информации;

СУБД – система управления базами данных;

ТЗИ – техническая защита информации.

II. Термины и определения

Для целей настоящей Концепции используются следующие основные термины и определения:

автоматизированная система (обработки информации) – организационно-техническая система, представляющая собой совокупность взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей потребителей информации. АС является разновидностью информационной системы;

головное общество – АО «ОСК» – юридическое лицо, которое входит в интегрированную структуру оборонно-промышленного комплекса и имеет возможность определять решения, принимаемые остальными юридическими лицами;

ГосСОПКА – единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

документ – материальный носитель информации с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, имеющий реквизиты, позволяющие его идентифицировать, и предназначенный для передачи информации во времени и в пространстве в целях ее общественного использования и хранения;

документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель;

доступ к информации – возможность получения информации и ее использования;

доступность информации – способность информации обеспечивать своевременный беспрепятственный доступ к ней субъектов, имеющих на это надлежащие полномочия;

защита информации – принятие правовых, организационных и технических мер, направленных на: обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных

неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации;

защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями локальных нормативных актов АО «ОСК» или требованиями, устанавливаемыми собственником информации;

иностранная техническая разведка – деятельность иностранного государства по добыванию разведывательной информации с помощью технических систем, средств и аппаратуры;

информация – сведения о лицах, предметах, событиях, явлениях и процессах, независимо от формы их представления;

информационная безопасность – процесс обеспечения конфиденциальности, целостности и доступности информации, а также устойчивого функционирования информационной системы в условиях реализации угроз;

информационная инфраструктура – взаимосвязанная совокупность информационных систем и подсистем;

информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов, файлов в информационных системах (библиотеках, архивах, фондах, банках данных, других видах информационных систем);

информационная сфера (среда) – совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений;

информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами или локальными нормативными актами АО «ОСК»;

инцидент информационной безопасности – одно или несколько нежелательных или неожиданных событий ИБ, которые с высокой степенью вероятности могут привести к компрометации в бизнес-процессах и создают угрозы для информационной безопасности;

кибербезопасность – меры безопасности, применяемые для защиты от уязвимостей, возникающих в результате ненадлежащей эксплуатации,

интеграции, обслуживания и проектирования компьютеризированных систем, и от преднамеренных и непреднамеренных угроз ИБ;

компьютерный инцидент – вид инцидента ИБ, факт нарушения или прекращения функционирования информационной системы, нарушения безопасности обрабатываемой информации, в том числе произошедший в результате компьютерной атаки;

конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

общества Группы ОСК (общества) – общества, в которых АО «ОСК» в силу преобладающего участия в их уставных капиталах и в соответствии с заключенными между ними договорами либо иным образом имеет возможность влиять на принимаемые этими обществами решения в области научно-технической, инвестиционной, производственно-технической, финансовой, ценовой, сбытовой, социальной и кадровой политики в соответствии с законодательством Российской Федерации и учредительными документами указанных обществ;

объект защиты – обобщенное понятие, используемое в настоящей Концепции для обозначения объекта, в отношении которого осуществляется деятельность по защите информации. К таким объектам относятся: информация, информационные системы, технические средства, программное обеспечение, средства защиты информации, помещения и другие объекты капитального строительства;

объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров;

объект КИИ – информационная система, информационно-телекоммуникационная сеть, автоматизированная система управления субъекта КИИ;

охраняемые сведения – сведения, составляющие государственную тайну, связанные с созданием, эксплуатацией и ликвидацией образца ВВТ или объекта капитального строительства, которые могут быть получены в процессе ведения ИТР;

противодействие иностранным техническим разведкам – деятельность, направленная на исключение или затруднение получения иностранными техническими разведками охраняемых сведений;

событие информационной безопасности – выявленное (идентифицированное) появление определенного состояния системы, сервиса или сети, указывающее на возможное нарушение политики обеспечения ИБ, отказ защитных мер или возникновение ранее неизвестной ситуации, которая может иметь отношение к вопросам ИБ;

средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации;

субъекты КИИ – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей;

техническая защита информации – обеспечение защиты (некриптографическими методами) информации ограниченного доступа, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;

угроза безопасности информации – случайное (неумышленное) или преднамеренное (злоумышленное) воздействие, приводящее к нарушению целостности, доступности и конфиденциальности информации или поддерживающей ее инфраструктуры, которое наносит ущерб собственнику, распорядителю или пользователю информации. Это также

потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации и неправомерному ее тиражированию. Кроме того, это фактор или совокупность факторов, создающих опасность функционированию и развитию информационной среды;

уровень защиты (класс, категория защищенности) – характеристика, описываемая в нормативных документах определенной группой требований к данному классу и категории защищенности;

уязвимость информационной системы – недостаток системы, использование которого может привести к реализации угроз ИБ (нанести ущерб информационной системе);

целевая компьютерная атака – целенаправленное воздействие злоумышленников на информационную систему с помощью программно-аппаратных средств в целях нарушения или прекращения их функционирования или создания угрозы безопасности обрабатываемой информации;

целостность информации – свойство информации, при котором отсутствует любое ее изменение (по отношению к некоторому фиксированному состоянию информации) либо оно осуществляется только преднамеренно субъектами, имеющими на него право.

III. Общие положения

Концепция информационной безопасности АО «ОСК» и обществ Группы ОСК (далее – Концепция) представляет собой принятую единую систему взглядов на решение в АО «ОСК» и обществах Группы ОСК проблем обеспечения информационной безопасности.

Концепция подлежит обязательному применению в АО «ОСК» и обществах Группы ОСК, которые присоединились к нему путем принятия соответствующего решения единоличным органом управления общества, имеющим необходимые полномочия согласно нормам законодательства Российской Федерации и учредительным документам.

АО «ОСК» является интегрированной структурой оборонно-промышленного комплекса, акционерным обществом с государственным участием, компанией холдингового типа, объединяющей проектно-конструкторские бюро, судостроительные, судоремонтные, машиностроительные, электротехнические и другие предприятия, в целом участвующие в работах по созданию образцов ВВТ в рамках выполнения заданий государственного оборонного заказа и судов гражданского назначения.

На основании Указа Президента Российской Федерации от 9 октября 2023 г. № 753 «Об управлении находящимися в федеральной собственности акциями акционерного общества «Объединенная судостроительная корпорация» сто процентов акций АО «ОСК» переданы в доверительное управление Банку ВТБ (ПАО) сроком на пять лет.

В Концепции изложены общие свойства информационной сферы АО «ОСК» и обществ Группы ОСК и объектов обеспечения информационной безопасности, определены основные угрозы безопасности информации, принципы организации мероприятий по ее защите, особенности защиты различных видов тайн.

Настоящая Концепция разработана в соответствии с требованиями законодательства Российской Федерации о защите различных видов тайн, нормативных правовых актов в области информационной безопасности, руководящих и нормативно-методических документов ФСТЭК России и ФСБ России.

Система взглядов, изложенная в Концепции, базируется на качественном осмыслении вопросов ИБ, не акцентирует внимание на количественном анализе рисков и обосновании затрат, необходимых для защиты информации.

В Концепции не рассматриваются вопросы охраны зданий и помещений, обеспечения их сохранности и физической целостности, защиты от стихийных бедствий, сбоев в системах энергоснабжения и другие вопросы, косвенно влияющие на обеспечение ИБ.

Положения Концепции адресованы работникам АО «ОСК» и обществ Группы ОСК, взявшим на себя обязательства либо обязанным по своему статусу исполнять функционал по организации, осуществлению или обеспечению защиты информации.

Решение задач обеспечения информационной безопасности в АО «ОСК» и обществах Группы ОСК достигается путем формирования системы локальных нормативных актов и организационно-распорядительных документов по защите информации, разрабатываемых с учетом положений настоящей Концепции и не противоречащих им.

IV. Особенности информационной сферы

Информационная сфера АО «ОСК» и обществ Группы ОСК имеет следующие особенности:

а) на функционирование информационной среды оказывают влияние следующие обстоятельства:

наличие управляющей компании (головного общества) и большого количества обществ Группы ОСК;

распределенность обществ по территории Российской Федерации;

разделение обществ по специализации: проектные бюро, судостроительные, судоремонтные и иные организации;

высокая интенсивность информационных потоков как внутри обществ Группы ОСК, так и с внешними абонентами (органами власти, государственными и коммерческими российскими и зарубежными организациями);

б) информационные потоки с внешними органами и организациями, между обществами и внутри них образуют единое информационное пространство, в котором циркулирует информация, в том числе содержащая сведения, составляющие различные виды тайн, и принадлежащая различным обладателям информации;

в) в обществах циркулирует, обрабатывается и хранится преимущественно следующая информация:

информация, содержащая сведения, составляющие государственную тайну, – в связи с предоставленным обществам правом на осуществление работ с использованием сведений, составляющих государственную тайну;

информация, содержащая сведения, составляющие служебную тайну органов государственной власти Российской Федерации, – в связи с участием обществ в исполнении отдельных государственных функций;

информация, содержащая сведения, составляющие служебную тайну в области обороны, – в связи с участием обществ в исполнении функций по организации и реализации мероприятий в области обороны, распространение которых может нанести вред Российской Федерации;

информация, содержащая сведения, составляющие коммерческую тайну (как собственно обществ, так и иных организаций), – в связи с деятельностью на рынке товаров (работ, услуг);

информация, содержащая отдельные сведения о физических лицах, – в связи с необходимостью обработки персональных данных;

информация, не отнесенная к информации ограниченного доступа, используемая в ходе основной деятельности обществ (в том числе управления технологическими, производственными или иными процессами), неограниченное распространение или модификация которой может создать угрозы информационной безопасности, нарушения функционирования ИС, физической безопасности обществ, нанести репутационный или иной значимый ущерб. К такой информации могут относиться: сообщения (архивы) электронной почты, телефонные справочники, сведения о договорной работе,

использовании производственного и технологического оборудования, экологически вредных производствах, аварийно-опасных или взрывоопасных объектах, структурах, программно-аппаратных составах и пользователях ИС, а также информация, циркулирующая в средствах защиты информации и средствах физической защиты;

иная общедоступная информация – в связи с необходимостью использования в деятельности общеизвестных сведений и иной информации, доступ к которой не ограничен законодательством Российской Федерации;

г) субъектами правоотношений в информационной сфере обществ, будучи обладателями перечисленных основных видов информации ограниченного доступа, являются:

Российская Федерация, субъекты Российской Федерации, муниципальные образования соответственно через государственные органы, их подведомственные организации, органы местного самоуправления, муниципальные организации как обладатели информации, содержащей сведения, составляющие государственную, служебную тайну и служебную тайну в области обороны;

юридические лица, в том числе общества как обладатели информации, содержащей сведения, составляющие коммерческую тайну;

физические лица как субъекты персональных данных;

д) выделяются два вида объектов информатизации, используемых для обработки (обсуждения) информации ограниченного доступа: объекты вычислительной техники и так называемые выделенные (защищаемые) помещения.

К объектам вычислительной техники относятся: АС, ИС, автоматизированные рабочие места, вычислительные сети и системы передачи данных, средства изготовления и размножения документов и другие отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

К выделенным (защищаемым) помещениям относятся помещения (служебные кабинеты, переговорные комнаты, конференц-залы), специально предназначенные для обсуждения или воспроизведения информации ограниченного доступа, в том числе с использованием технических средств и систем (средств специальной связи, систем звукоусиления и иных);

е) исходя из положений Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» большинство обществ являются субъектами КИИ и используют в своей деятельности объекты КИИ, к которым могут быть отнесены:

локальные вычислительные сети;

ИС, предназначенные для разработки и хранения конструкторской документации;

испытательные стенды;

системы цифрового моделирования;

ИС управления хозяйственной деятельностью, реализующие функции стратегического планирования (BPM-системы, OLAP-системы);

ИС управления ресурсами, позволяющие осуществлять планирование, учет и анализ ресурсов (ERP-системы);

ИС, обеспечивающие управление жизненным циклом продукции (PLM-системы);

ИС управления производственными ресурсами в ходе технологического процесса (MES-системы);

АС, обеспечивающие контроль и (или) управление технологическим и (или) производственным оборудованием (исполнительными устройствами) и реализованными на нем технологическими или производственными процессами (SCADA-системы, распределенные системы управления);

информационные (автоматизированные) системы управления станками с числовым программным управлением.

В объектах КИИ могут циркулировать любые виды информации, перечисленные в пункте «в» настоящего раздела;

ж) в связи с производственной необходимостью многие ИС обществ являются территориально распределенными, имеют сложную архитектуру и используют сети связи общего пользования. В интересах реализации бизнес-процессов к ИС организован удаленный доступ из вычислительных сетей обособленных подразделений и отдельно расположенных АРМ работников обществ, а также сторонних организаций в рамках выполнения договорных отношений;

е) в большинстве ИС обществ используются средства вычислительной техники, системное и прикладное ПО иностранного производства. Введенные санкции в отношении Российской Федерации привели к отзыву лицензий и (или) прекращению технической поддержки импортных ПО, вычислительной техники, сетевого оборудования, средств защиты информации, что может приводить к их полному отключению или постоянной деградации уровня защиты из-за отсутствия обновлений безопасности. С другой стороны, продолжение технической поддержки (обновления ПО) иностранными организациями создает риски внедрения вредоносного кода с деструктивными последствиями.

V. Угрозы информационной безопасности

По направленности воздействия угрозы информационной безопасности АО «ОСК» и обществам Группы ОСК подразделяются на угрозы, нарушающие:

конфиденциальность информации;

целостность информации;

доступность информации.

В информационных системах нарушение доступности информации может проявляться в виде:

отказа в предоставлении информации (в обслуживании);

нарушения функционирования системы, создания нештатных режимов работы программно-аппаратных средств;

несанкционированного использования системы.

По степени воздействия на информационную среду угрозы подразделяются на пассивные и активные. При реализации пассивных угроз структура и содержание информационной среды не изменяются, при осуществлении активных угроз такие изменения происходят.

По типу источника угрозы подразделяются на:

антропогенные, обусловленные преднамеренными или непреднамеренными действиями человека;

техногенные, обусловленные техническими средствами в процессе технократической деятельности человека;

стихийные, обусловленные природными явлениями.

По расположению источника угроз по отношению к информационной среде угрозы подразделяются на внешние и внутренние.

Внешними источниками угроз могут быть:

деятельность иностранных государств, иностранных и отечественных организаций;

деятельность физических лиц, в том числе физических лиц, объединенных в неформальные сообщества (группы, хакерские группировки);

действия криминальных структур;

природные стихийные явления и техногенные катастрофы.

Внутренними источниками угроз являются:

нарушения работниками установленных правил сбора, обработки и передачи информации и иных требований ИБ;

ошибки обслуживающего персонала;

отказы и неисправности (сбои) технических и программных средств обработки, хранения, передачи данных и защиты информации;

отказы и неисправности технических и программных средств контроля эффективности принятых мер по защите информации.

По способам реализации угроз безопасности информации выделяются:

угрозы утечки информации по техническим каналам;

угрозы, связанные с несанкционированным доступом.

Угрозы утечки информации по техническим каналам описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки данных.

К наиболее актуальным и опасным угрозам ИБ, связанным с несанкционированным доступом, в настоящее время относятся целенаправленные атаки на информационные активы и информационную инфраструктуру обществ, а также продолжение использования средств вычислительной техники, ПО и средств защиты информации иностранного производства.

Угроза, связанная с НСД, в информационных (автоматизированных) системах может быть реализована за счет:

непосредственного обращения (проникновения) к объектам доступа;

модификации средств защиты информации, позволяющей реализовать угрозы информационной безопасности;

уязвимостей нулевого дня в системном и прикладном программном обеспечении;

создания/модификации программных и технических средств с целью обхода средств защиты;

внедрения в ИС программ-вирусов, а также иных программных или технических средств, нарушающих ее функции.

Массовое использование в деятельности обществ сетей связи общего пользования, в том числе информационно-телекоммуникационной сети Интернет, повышает риски реализации угроз ИБ в отношении ИС, в том числе посредством проведения целевых компьютерных атак. Большинство кибератак осуществляется в целях несанкционированного доступа к информационным ресурсам.

Основными способами таких атак являются:

анализ трафика. Осуществляется за счет прикладных программ, перехватывающих все сетевые пакеты, – анализаторов трафика. Ввиду того что некоторые сетевые приложения передают данные в незашифрованном виде (Telnet, FTP, SMTP, POP3 и т.д.), с помощью анализатора трафика возможен несанкционированный доступ к информации конфиденциального характера (в том числе имена пользователей и пароли);

подмена IP-адреса. Осуществляется путем имитирования действий легального пользователя в интересах получения сетевых пакетов и отправки

ответов на них с ложной информацией или вредоносными командами. Для этого используются IP-адреса в пределах диапазона разрешенных в ИС IP-адресов или авторизованные внешние адреса, которым разрешается доступ к определенным сетевым ресурсам;

отказ в обслуживании (Denial of Service, DoS). Является наиболее известной и несложной в реализации формой атак. Атаки DoS не нацелены ни на получение доступа к ИС, ни на получение какой-либо информации, но атака DoS делает ИС или серверные приложения недоступными для использования за счет превышения допустимых пределов функционирования сети (перегрузки запросами или командами), операционной системы или приложения. Некоторые атаки сводят к нулю производительность сети, переполняя ее нежелательными и ненужными пакетами или сообщая ложную информацию о текущем состоянии сетевых ресурсов;

DDoS-атаки (Distributed Denial Of Service Attack). Разновидность атаки DoS, только DDoS-атаки проводятся с двух и более хостов. Злоумышленники искусственно создают лавинообразный рост запросов к онлайн-ресурсу, чтобы увеличить на него нагрузку и вывести его из строя. Обнаружить DDoS-атаки значительно сложнее, потому что запросы выглядят «живыми» и вызывают меньше подозрений. При этом DDoS-атаки дают возможность отправлять большие объемы трафика в целевую сеть;

взлом пароля. Проводится с помощью целого ряда методов, таких как полный перебор, применение вредоносного программного обеспечения, подмена IP-адреса и анализ трафика. Зачастую используются специальные программы для подбора паролей пользователей с различными привилегиями и осуществления доступа к ресурсам ИС;

атаки MITM («человек посередине», Man-in-the-Middle). В этой атаке злоумышленник тайно ретранслирует и при необходимости подменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом. Для атак MITM часто используются анализаторы трафика, транспортные протоколы и протоколы маршрутизации. Проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии;

атаки на уровне приложений. Реализуются с использованием уязвимостей серверного программного обеспечения (sendmail, HTTP, FTP) и приложений в целях получения доступа к АРМ от имени пользователя, работающего с приложением (обычно атакам подвергаются привилегированные администраторы с правами системного доступа). Часто используются порты,

которым разрешен проход через межсетевые экраны. Получая доступ к приложению, злоумышленник может не только деактивировать его работу, но и завладеть ценной информацией, что грозит финансовыми и репутационными рисками;

сетевая разведка. Проводится в целях сбора информации о сети с помощью общедоступных данных и приложений в форме запросов DNS, эхо-тестирования и сканирования портов. Запросы DNS помогают понять, кто владеет доменом и какие адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде, список поддерживаемых ими сервисов и характеристик используемых приложений. Результаты сетевой разведки используются при подготовке других видов атак против ИС;

переадресация портов. Используется для организации проникновения в ИС посредством перенаправления сетевых пакетов со взломанного хоста внутрь ИС путем преодоления шлюза (маршрутизатора, межсетевого экрана);

использование уязвимостей нулевого дня. Нулевым днем называют день, когда стало известно о какой-то уязвимости, которую хакеры уже использовали. Поскольку уязвимости нулевого дня заранее неизвестны, не обнаруживаются классическими антивирусными технологиями, то на случай их использования нет готовых защитных механизмов, что делает такие уязвимости очень опасными и способными нанести вред ИС. Пока уязвимость неизвестна разработчикам ПО и не устранена, злоумышленники могут долго и незаметно проводить скрытые целевые атаки посредством внедрения вредоносного кода (вредоносных программ);

внедрение вредоносного кода/программ (вирусов, шифровальщиков, троянских или иного программного кода), предназначенных для осуществления несанкционированного доступа к информации или воздействия на информацию или ресурсы ИС. Троянская программа – программа, которая содержится в полезном приложении или файле и выполняет вредоносные действия без ведома пользователя. Шифровальщик – вредоносная программа-вымогатель, шифрующая файлы на машинных носителях информации, сетевых дисках, в облачных хранилищах и требующая у пользователя выкуп за их расшифровку.

В ходе реализации мероприятий по цифровой трансформации необходимо учитывать следующие особенности информационной инфраструктуры обществ, которые могут оказать влияние на реализацию угроз информационной безопасности:

инфраструктуры многих обществ являются территориально распределенными, построенными и функционирующими с использованием

разнообразных, а в ряде случаев устаревших типов программно-аппаратных средств и информационных технологий;

применяемое системное и прикладное ПО, в том числе СУБД, САПР, преимущественно иностранного происхождения ввиду отсутствия качественных отечественных аналогов;

порядок обновления различных версий используемого ПО не исключает внедрения вредоносного кода/программ;

при осуществлении миграции данных из старых ИС возможны уничтожение или модификация информации;

большинство ИС не создавались в защищенном исполнении, а для их защиты используются «наложенные» средства защиты информации;

отсутствует единая защищенная среда выполнения корпоративных информационных процессов;

информационный обмен осуществляется разнородными способами как по незащищенным каналам связи, так и с использованием средств криптографической защиты информации;

укомплектованность многих обществ специалистами по обеспечению информационной безопасности и уровень подготовки специалистов не соответствуют современным угрозам;

вследствие использования разнородных программно-аппаратных средств, технологических процессов, сервисов и инструментов ИБ (средств защиты информации), отсутствия единого подхода к автоматизации и осуществлению мониторинга процессов обеспечения безопасности информации события ИБ являются непрозрачными для мониторинга и реализации единой политики информационной безопасности на уровне головного общества.

VI. Основные принципы обеспечения информационной безопасности

В АО «ОСК» и обществах Группы ОСК должны соблюдаться следующие принципы обеспечения информационной безопасности:

а) неотъемлемость. Безопасность объектов защиты является их неотъемлемым свойством (характеристикой), а не дополнительным сервисом. Соблюдение требований ИБ должно быть обязательным для всех работников общества, а также работников контрагентов, имеющих доступ к объектам защиты общества, и являться частью корпоративной культуры общества;

б) комплексность. Необходимо согласованное применение разнородных средств при построении целостной системы защиты информации, перекрывающей все направления реализации угроз ИБ и не содержащей слабых

мест на стыках отдельных ее компонентов. Защита должна обеспечиваться физическими средствами, организационными, технологическими и правовыми мерами, обеспечивающими в комплексе инженерно-техническую защиту объектов, защиту от несанкционированного доступа к компьютерам пользователей и серверам, разграничение доступа к информационным ресурсам, криптографическую защиту информации, защиту каналов обмена информацией, защиту информации от утечек по техническим каналам и т.д.;

в) системность. Деятельность по ИБ должна быть строго и всесторонне регламентирована. Политика ИБ общества как совокупность норм, требований, положений, порядков и инструкций должна учитывать все наиболее слабые и уязвимые места защищаемых объектов и охватывать весь их жизненный цикл. При этом необходим учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения защиты информации в ИС. Необходима оценка не только имеющихся, но и возможных в будущем сценариев реализации угроз;

г) интегрированность. Обеспечение ИБ – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты информации, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС, начиная с этапа проектирования, а не только на этапе эксплуатации;

д) адекватность. Применяемые методы и средства ЗИ должны быть адекватны угрозам уничтожения, утечки или искажения информации. Недопустима как недостаточная, так и чрезмерная защита. Создать абсолютно защищенную систему невозможно, в связи с этим при проектировании систем ЗИ следует соблюдать баланс между стойкостью защиты и ее стоимостью, потреблением вычислительных ресурсов, удобством работы пользователей и другими характеристиками систем ЗИ;

е) идентификация и оценка активов. Реализация принципа «адекватность» должна основываться на идентификации всех информационных активов и определении их ценности для целей и задач общества;

ж) гибкость и управляемость. Система ЗИ должна обеспечивать возможность варьировать уровень защищенности объектов. Гибкость управления и применения системы ЗИ избавляет от необходимости полной замены средств ЗИ на новые при смене условий функционирования защищаемых объектов. При выборе между организационными и техническими мерами приоритет должен отдаваться мерам технического характера;

з) своевременность. Разработка мер ЗИ должна вестись вместе с разработкой объекта защиты. Неприемлем ввод объекта в эксплуатацию до обеспечения защиты. Разработка подсистемы безопасности, осуществляемая параллельно разработке объекта, оптимизирует затраты ресурсов и позволяет вырабатывать наиболее эффективные решения;

и) упреждение. Акцент в обеспечении ИБ должен делаться на предупредительных мерах, предотвращении событий ИБ, которые могут повлиять на конфиденциальность, целостность и доступность информации;

к) контролируемость. Должна обеспечиваться своевременность выявления и пресечения попыток нарушения установленных требований и правил ИБ. Постоянный контроль ИБ, выявление и устранение уязвимостей, мониторинг событий, влияющих на ее состояние, является обязательной составляющей эффективной системы организации и управления ЗИ;

л) законность. Деятельность по ИБ должна осуществляться в соответствии с законодательством, требованиями надзорных и контролирующих органов, нормативными актами в области ИБ;

м) следование лучшим практикам. При реализации мер ЗИ рекомендуется учитывать требования российских и международных стандартов в области ИБ как лучших практик;

н) анализ и совершенствование. Необходима постоянная работа по оценке эффективности и совершенствованию мер и средств ЗИ на основе анализа функционирования информационных систем, изменений в методах и средствах перехвата информации и воздействия на компоненты систем, изменений нормативных требований по защите и опыта работы в области ИБ;

о) минимизация полномочий. Предоставление пользователям прав доступа определяется исключительно производственной необходимостью. Доступ к информации должен предоставляться только в том случае и в том объеме, в каком это минимально необходимо работнику для выполнения его должностных обязанностей;

п) разделение функций. При определении состава ролей, использующихся для распределения прав доступа, следует исключить концентрацию полномочий, совмещение в рамках одной роли такого состава функций, которое позволило бы одному работнику единолично осуществлять выполнение критичных операций или получать полный и неконтролируемый доступ к какому-либо объекту защиты. Действия работников, обладающих полномочиями администраторов, должны находиться под особым контролем со стороны подразделения по ИБ;

р) персонификация. Для всех используемых учетных записей должна быть обеспечена возможность однозначно установить субъект, совершивший в определенный момент времени определенное действие с использованием этой учетной записи, в том числе для служебных учетных записей. В общем случае действия каждого работника общества должны осуществляться от имени одной персонифицированной учетной записи. Необходимо использование единственной учетной записи каждым работником поскольку наличие у работника двух и более учетных записей (по крайней мере в рамках одного домена) делает неэффективной систему распределения и контроля полномочий. Исключение по решению руководства общества могут составлять, например, администраторы систем, должностные обязанности которых предполагают внесение изменений в указанные системы. Для них в дополнение к учетной записи со стандартными правами пользователя может быть создана учетная запись администратора с расширенными полномочиями. Наличие не закрепленных за субъектами доступа учетных записей не допустимо;

с) запрещено все, что не разрешено. Доступ к любому защищаемому объекту должен предоставляться только при наличии соответствующего разрешения (правила, настройки СЗИ) на основании локальных нормативных актов общества. Любой доступ, не разрешенный явно, должен быть запрещен. Такой подход обеспечивает только известные безопасные действия и освобождает от необходимости распознавать любую угрозу, что очень ресурсоемко и неэффективно;

т) стойкость СЗИ. Уровень стойкости применяемых средств и эффективность мер ЗИ должны определяться ценностью защищаемого объекта и требовать от злоумышленника неадекватно больших затрат времени и вычислительных мощностей на их преодоление;

у) эшелонированность СЗИ. Нельзя полагаться на защиту на одном уровне информационной инфраструктуры, какой бы надежной она ни считалась. Необходимо организовать защиту на разных уровнях информационной инфраструктуры;

ф) разнообразие СЗИ. В целях снижения зависимости уровня безопасности общества от поставщиков, контрагентов, партнеров, а также сбоев и отказов отдельных систем целесообразно использовать СЗИ различных производителей;

х) специализация и профессионализм. К работам по созданию, внедрению и сопровождению СЗИ и реализации мер ЗИ в рамках аутсорсинга необходимо привлекать специализированные организации, наиболее подготовленные к конкретному виду деятельности по обеспечению

безопасности информационных ресурсов, имеющие опыт практической работы, необходимые лицензии на право оказания услуг в этой области, обладающие партнерскими статусами компаний-вендоров внедряемых решений и имеющие в своем штате высококвалифицированный персонал.

Требования к внешним контрагентам, выполняющим указанные функции, а также порядок взаимодействия и распределения ответственности между ними определяются в документах закупки и соответствующих договорах, подлежащих согласованию с ДБ. Реализация организационных мер и эксплуатация средств ЗИ должна осуществляться работниками, обладающими соответствующими компетенциями. Предоставление и администрирование на общесистемном уровне средств вычислительной техники, необходимых для функционирования средств ЗИ, должны осуществляться подразделениями по информационным технологиям. Для эффективного применения организационных и технических мер ЗИ руководством на всех уровнях должны выделяться необходимые и достаточные ресурсы;

ц) осведомленность. Осведомленность работников и контрагентов в вопросах ИБ – обязательное условие безопасного функционирования объектов защиты общества;

ч) персональная ответственность. Ответственность за обеспечение безопасности информации и систем ее обработки возлагается на каждого работника общества в пределах его полномочий;

ш) лояльность персонала. Необходимо создание такой благоприятной атмосферы в коллективах всех подразделений общества, при которой выполнение требований ИБ воспринималось бы работниками как осознанная необходимость и неотъемлемая часть корпоративной этики;

щ) вовлеченность руководства. Руководитель общества несет персональную ответственность за обеспечение ИБ. До руководства общества на регулярной основе в порядке, установленном отдельными локальными нормативными актами общества, доводится информация о достигнутых результатах, имеющихся системных проблемах и стратегических потребностях общества в области ИБ. На уровень руководства общества при необходимости могут быть делегированы риски ИБ, инциденты ИБ и иные проблемы ИБ;

ы) взаимодействие и координация. Эффективное обеспечение ИБ достигается только при условии взаимодействия и координации как между всеми структурными подразделениями общества, так и при взаимодействии с головным обществом и такими организациями, как Центр мониторинга и реагирования на компьютерные атаки, Федеральная служба по

техническому и экспортному контролю, Федеральная служба безопасности Российской Федерации, Министерство внутренних дел Российской Федерации и другие профильные министерства и ведомства.

VII. Организация обеспечения информационной безопасности

Соблюдение прав и законных интересов субъектов правоотношений в информационной сфере обеспечивается посредством принятия в обществах правовых, организационных и технических мер, соответствующих установленным уровням защиты, направленных на:

обеспечение конфиденциальности информации ограниченного доступа;

обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении информации (обеспечение целостности информации);

реализацию прав доступа к информации (обеспечение доступности информации);

минимизацию негативных последствий инцидентов ИБ;

обеспечение бесперебойного функционирования информационных систем и других объектов КИИ.

В информационной сфере АО «ОСК» и обществ Группы ОСК защите от угроз безопасности информации подлежат:

документированная информация, в том числе на электронных носителях, содержащая сведения, составляющие государственную тайну, или иные сведения конфиденциального характера, определенные Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

данные, хранящиеся в объектах вычислительной техники и содержащие сведения, составляющие государственную тайну, или иные сведения конфиденциального характера;

речевая информация, содержащая сведения, составляющие государственную тайну, или иные сведения конфиденциального характера;

охраняемые сведения об образцах ВВТ;

охраняемые сведения об объектах капитального строительства обществ;

другие виды информации, указанные в пункте «в» раздела IV настоящей Концепции.

Исходя из этого, основными направлениями деятельности (процессами) по обеспечению ИБ в обществах являются:

противодействие иностранным техническим разведкам и техническая защита информации в целях защиты сведений, составляющих государственную

тайну, об образцах ВВТ, объектах капитального строительства, а также информации, циркулирующей в образцах ВВТ (при установлении таких требований заказчиком);

противодействие иностранным техническим разведкам и техническая защита информации, составляющей государственную тайну (в рамках объектовой защиты обществ);

техническая защита информации ограниченного доступа, не составляющей государственную тайну;

обеспечение безопасности объектов КИИ;

обеспечение информационной безопасности информационной инфраструктуры обществ, в том числе обнаружение, предупреждение, ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты (противодействие кибератакам);

обеспечение целостности и доступности общедоступной информации.

Общества, участвующие в выполнении государственного оборонного заказа, осуществляют деятельность по противодействию иностранным техническим разведкам в целях защиты охраняемых сведений об образцах ВВТ, а также объектах капитального строительства. Охраняемые сведения определяются заказчиками в технических заданиях на создание объектов защиты или на иные виды работ с ними. Деятельность по ПД ИТР необходима в тех случаях, когда носителями сведений об объектах защиты от ИТР являются физические поля и (или) физико-химические свойства объектов защиты, в которых эти сведения находят свое отображение в виде количественных и качественных характеристик физико-химических проявлений объектов защиты, технических решений и процессов. Такая деятельность осуществляется путем проведения организационных и технических мероприятий во взаимосвязи с режимными и другими мероприятиями по обеспечению информационной безопасности.

Техническая защита информации осуществляется техническими, программными и программно-техническими методами в отношении информации, обрабатываемой, циркулирующей и (или) хранящейся в объектах информатизации и технических средствах образцов ВВТ.

В целях защиты информации при передаче по каналам связи и (или) защиты информации от несанкционированного доступа при ее обработке и хранении, а также защиты от навязывания ложной информации дополнительно могут использоваться средства криптографической защиты информации.

При создании судов в обществах Группы ОСК необходимо осуществлять деятельность по обеспечению киберустойчивости устанавливаемых судовых

компьютеризированных (информационных) систем. Рекомендации по проектированию, изготовлению, обслуживанию и проведению испытаний судовых компьютеризированных систем, а также рекомендации к системам управления безопасностью судов определены в Руководстве по обеспечению кибербезопасности Российского морского регистра судоходства (НД № 2-030101-040).

Отдельным направлением в области обеспечения ИБ в обществах (субъектах КИИ) является создание систем безопасности значимых объектов КИИ и обеспечение их бесперебойного функционирования в соответствии с требованиями Федерального закона от 26 июля 2017 г. № 187-ФЗ, Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127, нормативных методических документов регуляторов (ФСТЭК России и ФСБ России), отдельных указаний и рекомендаций Минцифры России, Минпромторга России и НКЦКИ. Формирование перечней объектов КИИ, подлежащих категорированию, и присвоение им одной из категорий значимости осуществляется постоянно действующими комиссиями по категорированию обществ. Системы безопасности включают силы и используемые ими средства обеспечения безопасности значимых объектов КИИ и должны обеспечивать:

предотвращение неправомерного доступа к информации, обрабатываемой значимыми объектами КИИ, ее уничтожения, модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимых объектов КИИ;

восстановление функционирования значимых объектов КИИ, в том числе за счет создания и хранения резервных копий;

непрерывное взаимодействие с ГосСОПКА (НКЦКИ).

Указом Президента Российской Федерации от 30 марта 2022 г. № 166 установлены ограничения субъектам КИИ на осуществление закупок иностранного программного обеспечения, в целях его использования на принадлежащих им значимых объектах КИИ, а также закупок услуг, необходимых для использования этого ПО, на таких объектах. С 1 января 2025 г. субъектам КИИ запрещено использование иностранного ПО на принадлежащих им значимых объектах КИИ.

Нарастающая интенсивность незаконной деятельности злоумышленников по осуществлению попыток реализации угроз безопасности информации в ИС, в том числе посредством кибератак по каналам связи и сети Интернет, также требует разработки и принятия эффективных организационных и технических мер противодействия, направленных на мониторинг событий ИБ, обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

Организация деятельности по информационной безопасности осуществляется генеральным директором общества.

Кроме того, в соответствии Указом Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» в обществах, являющихся субъектами КИИ, на генерального директора общества возлагается персональная ответственность за обеспечение ИБ, в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагированию на компьютерные инциденты, а полномочия по обеспечению ИБ – на заместителя генерального директора по безопасности (при отсутствии в обществе такой должности – непосредственно на генерального директора).

Планирование, разработка и организация выполнения работ по ИБ осуществляются структурным подразделением, уполномоченным в области ИБ, подчиненным заместителю руководителя по безопасности (при отсутствии в обществе такой должности – генеральному директору). В порядке исключения возможно возложение функций по защите информации, не составляющей государственную тайну, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, на структурное подразделение по ПД ИТР и ТЗИ с разделением этих функций по разным работникам. Возложение указанных функций на иные подразделения, а также подчинение подразделения по ИБ заместителям генерального директора по другим направлениям деятельности не допускается.

Структура и функционал подразделения по ИБ должны соответствовать типовым, разработанным головным обществом. Количество работников подразделения по ИБ определяется руководством общества исходя из объема возложенных задач и должно обеспечивать эффективную реализацию всего комплекса мер по ИБ с учетом появления новых угроз безопасности информации, способов и методов проведения кибератак.

При выборе средств защиты информации следует учитывать, что:

для защиты сведений, составляющих государственную тайну, служебную тайну или служебную тайну в области обороны, используются средства защиты информации, сертифицированные по требованиям безопасности информации;

для защиты сведений, составляющих коммерческую тайну, или персональных данных используются средства защиты информации, сертифицированные по требованиям безопасности информации либо прошедшие в установленном порядке процедуру оценки соответствия по требованиям безопасности информации.

Указом Президента Российской Федерации от 1 мая 2022 г. № 250 с 1 января 2025 г. запрещено использование средств защиты информации, произведенных в иностранных государствах, совершающих в отношении Российской Федерации, российских юридических и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, подконтрольные им либо аффилированные с ними.

VIII. Особенности защиты различных видов тайн

1. Особенности защиты государственной тайны.

Защита информации, содержащей сведения, составляющие государственную тайну, в обществах осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Полномочия головного общества по защите государственной тайны возникают в связи с заключенным между АО «ОСК» и Минпромторгом России договором об организации защиты сведений, составляющих государственную тайну.

Аналогичные полномочия обществ Группы ОСК обусловлены заключенными между ними и АО «ОСК» договорами об организации защиты сведений, составляющих государственную тайну.

В целях совершенствования в АО «ОСК» и обществах Группы ОСК деятельности по защите информации, содержащей сведения, составляющие государственную тайну, функционирует корпоративная система противодействия иностранным техническим разведкам и технической защиты информации с координирующей, методической и контрольной функциями головного общества.

Документом, закрепляющим принципы, механизмы, правила, нормы функционирования указанной корпоративной системы является Положение о системе противодействия иностранным техническим разведкам и технической защиты информации в АО «ОСК».

В обществах разрабатываются необходимые локальные нормативные акты, определяющие порядок и содержание мероприятий по защите информации, составляющей государственную тайну.

2. Особенности защиты сведений конфиденциального характера.

В целях правового закрепления прав и обязанностей, возникающих в процессе взаимной передачи сведений конфиденциального характера между АО «ОСК» и обществами Группы ОСК, а также с учетом осуществляемой головным обществом координации деятельности обществ в области информационной безопасности головным обществом утвержден Порядок организации защиты сведений конфиденциального характера в обществах Группы ОСК. Порядок определяет единые правила организации, осуществления и контроля выполнения мероприятий по обеспечению конфиденциальности информации ограниченного доступа, не отнесенной к государственной тайне.

В интересах регулирования договорных отношений с другими организациями, связанных со взаимной передачей, использованием и обеспечением конфиденциальности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, общества заключают соглашения о конфиденциальности. Подписание договора присоединения к единому порядку организации защиты сведений конфиденциального характера и реализация в обществе указанного порядка позволяет исключить необходимость заключения иных соглашений о конфиденциальности как с АО «ОСК», так и с обществами, заключившими с ним такой договор присоединения.

При определении мер безопасности информации, обрабатываемой в информационных системах, целесообразно использовать Методические рекомендации по организации защиты информации в обществах Группы ОСК, утвержденные головным обществом.

2.1. Особенности защиты служебной тайны.

Обязательства по защите информации, содержащей сведения, составляющие служебную тайну, возникают в связи с участием АО «ОСК» и обществ Группы ОСК в реализации органами государственной власти государственных полномочий, предоставленных им законодательством Российской Федерации.

В связи с этим при организации и осуществлении в обществах защиты сведений, составляющих служебную тайну, за основу принимается Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденное постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

Порядок организации защиты информации, содержащей сведения, составляющие служебную тайну, определяется локальными нормативными актами обществ.

На материальные носители (документы), содержащие сведения, составляющие служебную тайну, необходимо наносить ограничительную пометку «Для служебного пользования».

2.2. Особенности защиты служебной тайны в области обороны.

Обязательства по защите информации, содержащей сведения, составляющие служебную тайну в области обороны, возникают в связи с участием АО «ОСК» и обществ Группы ОСК в исполнении функций по организации и реализации мероприятий в области обороны, распространение которых может нанести вред Российской Федерации.

Основанием для отнесения сведений к служебной тайне в области обороны является их соответствие перечням сведений, подлежащих отнесению к служебной тайне в области обороны, утвержденным руководителями федеральных органов исполнительной власти или федеральных государственных органов, в которых федеральным законом предусмотрена военная служба.

Порядок обращения с документами и другими материальными носителями информации, содержащими сведения, составляющие служебную тайну в области обороны, и порядок их защиты определены Правилами обращения со сведениями, составляющими служебную тайну в области обороны, утвержденными постановлением Правительства Российской Федерации от 26 ноября 2021 г. № 2052.

Передача информации, содержащей сведения, составляющие служебную тайну в области обороны, с использованием информационных систем осуществляется при условии выполнения требований нормативных правовых актов Российской Федерации в области защиты информации. Не допускается раскрытие такой информации третьим лицам без санкции должностного лица организации (органа власти), ее предоставившей.

На материальные носители (документы), содержащие сведения, составляющие служебную тайну, необходимо наносить ограничительную пометку «Для служебного пользования» со ссылкой на пункт перечня сведений, подлежащих отнесению к служебной тайне в области обороны.

Особенности обращения и организации защиты информации, содержащей сведения, составляющие служебную тайну в области обороны, отражаются в локальных нормативных актах.

2.3. Особенности защиты коммерческой тайны.

Защита информации, содержащей сведения, составляющие коммерческую тайну, осуществляется в АО «ОСК» и обществах Группы ОСК в соответствии с законодательством Российской Федерации о коммерческой тайне.

Режим коммерческой тайны устанавливается в связи с необходимостью соблюдения экономических интересов каждого общества в отдельности и обществ Группы ОСК в целом, а также с принятием обществами обязательств по защите коммерческой тайны других организаций.

Доступ органов и организаций к информации, содержащей сведения, составляющие коммерческую тайну обществ, осуществляется в форме передачи и в форме предоставления.

Передача обществом информации, составляющей коммерческую тайну, контрагенту осуществляется на материальном носителе только на основании договора в объеме и на условиях, предусмотренных договором, включая условие о принятии контрагентом установленных договором (соглашением) мер по охране ее конфиденциальности.

Предоставление информации, составляющей коммерческую тайну, государственным органам и органам местного самоуправления осуществляется на материальном носителе по их мотивированному требованию в целях выполнения их функций.

Режим коммерческой тайны в обществах устанавливается путем:

организации порядка отнесения информации к перечню сведений, составляющих коммерческую тайну общества;

ограничения доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

учета лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

регулирования отношений по использованию работниками и контрагентами информации, составляющей коммерческую тайну, на основании трудовых и гражданско-правовых договоров соответственно;

нанесения на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием полного наименования общества и места нахождения;

применения средств и методов технической защиты информации, иных мер, не противоречащих законодательству Российской Федерации.

В обществах разрабатываются и утверждаются в установленном порядке локальные нормативные акты, определяющие порядок организации защиты информации, содержащей сведения, составляющие коммерческую тайну, и перечень сведений, составляющих коммерческую тайну.

2.4. Особенности защиты персональных данных.

Обязательства АО «ОСК» и обществ Группы ОСК по защите информации, содержащей ПДн физических лиц, могут возникать в связи с необходимостью обработки таких данных.

Общество становится оператором ПДн при одновременном выполнении следующих условий:

в соответствии с компетенцией общества определены и обоснованы цели обработки персональных данных, состав персональных данных, подлежащих обработке, типовые действия (операции), совершаемые с персональными данными;

обработка персональных данных осуществляется в автоматизированном режиме или без использования вычислительной техники, если она соответствует характеру действий, совершаемых с ее использованием;

персональные данные представлены на материальных носителях в виде, пригодном для автоматизированной обработки или в аналогичной по возможностям информационной системе – картотеке, других систематизированных собраниях.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков). При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

В обществах необходимо разработать локальный нормативный акт, определяющий политику в отношении обработки и защиты персональных данных, в котором в том числе указываются цели обработки ПДн. Такими целями, например, могут являться:

регулирование трудовых отношений с работниками;

предоставление работникам и членам их семей дополнительных гарантий и компенсаций, в том числе добровольного медицинского страхования,

негосударственного пенсионного обеспечения и других видов социального обеспечения;

исполнение обязанностей, возложенных законодательством Российской Федерации, в том числе связанных с представлением ПДн в государственные органы;

формирование служебных справочников и служебных адресных книг;

формирование кратких биографических данных с последующим их размещением на официальных сайтах обществ в информационно-телекоммуникационной сети Интернет;

подготовка, заключение, исполнение и прекращение договоров с контрагентами;

реализация прав и законных интересов общества в рамках ведения видов деятельности, предусмотренных уставом и иными локальными нормативными актами;

необходимость сбора сведений для обеспечения разового пропуска субъектов ПДн на территорию общества или в иных аналогичных целях.

Конфиденциальность ПДн в обществе как операторе персональных данных обеспечивается в соответствии с законодательством Российской Федерации в области персональных данных.

IX. Заключительные положения

В Концепции сформулированы основные взгляды и базовые подходы к ИБ в соответствии с особенностями осуществления АО «ОСК» и обществами Группы ОСК основных видов деятельности, на которые необходимо ориентироваться при организации работ по обеспечению безопасности информации и разработке локальных нормативных актов.

Разработка самостоятельных концепций информационной безопасности для отдельных обществ не требуется.

X. Порядок внесения изменений и контроль версий

Настоящая Концепция подлежит пересмотру по мере необходимости.

Организация работ по актуализации настоящей Концепции возлагается на структурное подразделение головного общества, уполномоченное в области информационной безопасности.