ОСК.СМК 00.207-2022

Приложение
УТВЕРЖДЕНА
приказом АО «ОСК»
от «17» 09 2022 г. № 282

Политика информационной безопасности АО «ОСК»

Санкт-Петербург

2022

Содержание

Список сокращений

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

АС – автоматизированная система;

ИБ – информационная безопасность;

ИС – информационная система;

ЛНА – локальный нормативный акт;

НСД – несанкционированный доступ;

ОРД – организационно-распорядительный документ.

I. Общие положения

1.1. Настоящая Политика информационной безопасности (далее – Политика) разработана в развитие Концепции информационной безопасности АО «ОСК» и обществ Группы ОСК (ОСК.КСМК 00.011-2022) с учетом требований законодательства Российской Федерации в области обеспечения ИБ.

1.2. Политика определяет позицию АО «ОСК» в отношении ИБ в Обществе, основные цели, направления и меры по достижению целей и соблюдение принципов информационной безопасности в ходе производственной деятельности АО «ОСК» как головной организации интегрированной структуры оборонно-промышленного комплекса.

1.3. В рамках Политики принимается, что:

информационные технологии играют важную роль в достижении бизнес-целей Общества;

в средствах информатизации Общества циркулирует как открытая, общедоступная информация, так и информация ограниченного доступа;

информация является ценным активом Общества, требующим защиты независимо от форм ее представления;

информационная сфера Общества сталкивается с широким спектром угроз ИБ как внутреннего, так и внешнего характера, реализация которых может привести к различному ущербу (финансовые и репутационные потери, юридические взыскания, дезорганизация и т.д.);

стратегической целью Общества в области ИБ является обеспечение внедрения и использования информационных технологий с учетом принимаемых рисков получения возможного ущерба от реализации угроз ИБ;

стратегической задачей в области ИБ является создание системы обеспечения ИБ, основанной на методологии управления рисками и учитывающей актуальные угрозы бизнес-процессам Общества, а также правовые требования по ИБ.

1.4. Ключевыми объектами защиты в Обществе в первую очередь являются: информационные системы и/или сервисы, а также объекты информатизации, предназначенные для обработки информации ограниченного доступа.

1.5. Соблюдение положений настоящей Политики является обязательным для работников Общества и его обособленных структурных подразделений, а также учитывается в отношениях АО «ОСК» с контрагентами (потребителями продукции, поставщиками, партнерами, консультантами, аутсорсерами, стажерами, практикантами и т.д.).

II. Цели политики

2.1. Основными целями Политики ИБ являются:

обеспечение единых подходов к обеспечению ИБ в структурных подразделениях Общества;

создание методологической основы для разработки локальных нормативных актов по ИБ;

определение форм участия руководства Общества в решении проблем ИБ.

2.2. Основными целями процесса обеспечения ИБ являются:

выполнение требований законодательства Российской Федерации по защите обрабатываемой информации ограниченного доступа, в том числе содержащей сведения, составляющие государственную тайну;

поддержание необходимого уровня ИБ в АО «ОСК», соответствующего требованиям нормативной базы, локальных нормативных актов и организационно-распорядительных документов (далее – локальные документы) в области ИБ;

создание условий для устойчивого, непрерывного и оперативного управления бизнес-процессами Общества;

предупреждение возможности реализации угроз информационным ресурсам и ИС;

обеспечение конфиденциальности информации;

обеспечение целостности, доступности и подлинности информации, характеризующиеся их защищенностью от возможных непреднамеренных и злоумышленных воздействий, модификации и уничтожения;

минимизация ущерба и времени восстановления содержания информационных ресурсов и работоспособности информационных систем в случае возможной реализации угроз.

III. Направления обеспечения ИБ

3.1. Стратегия обеспечения информационной безопасности Общества заключается в формировании, эксплуатации и совершенствовании системы скоординированной деятельности по руководству и управлению информационной безопасностью.

3.2. Руководство и управление информационной безопасностью осуществляются в ходе производственной деятельности и ориентированы на содействие достижению бизнес-целей Общества через обеспечение защищенности информационной сферы, при этом выбор способов и методов обеспечения ИБ должен осуществляться исходя из имеющихся и прогнозируемых рисков и угроз.

3.3. АО «ОСК» стремится обеспечить соответствие уровня управления информационной безопасностью не ниже 4 в соответствии с классификацией стандарта COBIT, приведенной в Модели зрелости управления ИБ (приложение).

3.4. Организация работ по обеспечению ИБ в Обществе строится на требованиях законодательства Российской Федерации, нормативных методических документов в области информационной безопасности.

3.5. Требования настоящей Политики реализуются на основании локальных документов Общества, разработанных с учетом особенностей бизнес-процессов Общества и принципов обеспечения информационной безопасности, изложенных в Концепции ИБ АО «ОСК» и обществ Группы ОСК.

IV. Основные меры по обеспечению ИБ

Деятельность по информационной безопасности в Обществе осуществляется путем реализации организационных и технических мер.

4.1. К первоочередным организационным мерам относятся:

4.1.1. Планирование мероприятий по ИБ.

4.1.2. Определение объектов защиты (информационных ресурсов, информационных систем, объектов информатизации).

4.1.3. Создание системы защиты информации, составляющей государственную тайну.

4.1.4. Организация системы обеспечения информационной безопасности объектов защиты, не участвующих в обработке сведений, составляющих государственную тайну.

4.1.5. Формирование и укомплектование подразделения по ИБ.

4.1.6. Определение и закрепление в локальных документах полномочий, обязанностей по ИБ и ответственности руководства Общества, администраторов безопасности и владельцев ИС, а также иных должностных лиц.

4.1.7. Классификация информационных ресурсов по степени рисков и угроз, которым подвергаются информационные активы при нарушении конфиденциальности, целостности и доступности.

4.1.8. Разработка и реализация локальных документов по ИБ.

4.1.9. Согласование основополагающих локальных документов в сфере информационных технологий, цифровизации и цифровой трансформации с заместителем генерального директора по безопасности.

4.1.10. Обеспечение соответствия мер требованиям нормативных методических документов по информационной безопасности, реализация рекомендаций ФСТЭК России и ФСБ России.

4.1.11. Переподготовка и повышение квалификации работников подразделений по ИБ, информирование и обучение иных работников Общества правилам обеспечения ИБ.

4.1.12. Определение моделей угроз, нарушителей ИС, способов и методов проведения компьютерных атак, перечня недопустимых событий и негативных последствий (ущерба).

4.1.13. Определение порядка реагирования на события и инциденты информационной безопасности.

4.1.14. Реализация принципа «минимизации полномочий», при котором пользователям предоставляется доступ к информационным ресурсам в минимально достаточном для работы объеме.

4.1.15. Регламентация правил и процедур безопасного администрирования информационных ресурсов и информационных систем, дополнительных средств обеспечения информационной безопасности.

4.1.16. Регламентация правил и процедур обновления операционных систем и прикладного программного обеспечения.

4.1.17. Реализация мер по снижению рисков информационной безопасности при внедрении новых информационных систем, а также при внесении изменений в существующие информационные системы.

4.1.18. Учет документов и информационных ресурсов, регистрация действий пользователей и администраторов информационных систем, контроль процессов предоставления доступа.

4.1.19. Определение порядка и реализация подключения к ИС технических средств подрядчиков и иных сторонних организаций.

4.1.20. Разработка правил предоставления информации органам государственной власти и сторонним организациям, а также передачи материалов средствам массовой информации, включая размещение на официальных сайтах и на иных ресурсах сети Интернет.

4.1.21. Подписание с работниками Общества обязательств о сохранении сведений конфиденциального характера.

4.1.22. Оформление соглашений о конфиденциальности со сторонними организациями, которым предоставляется доступ к информации конфиденциального характера.

4.2. К основным техническим мерам относятся:

4.2.1. Размещение объектов защиты (серверное, коммуникационное, сетевое оборудование, рабочие места и объекты информатизации) на охраняемой территории, в пределах Российской Федерации. Ограничение и разграничение физического доступа на территории и в помещения с объектами защиты.

4.2.2. Использование встроенных механизмов безопасности информационных систем и программного обеспечения, а также применение сертифицированных средств защиты информации (отечественного производства).

4.2.3. Предотвращение утечки информации по техническим каналам.

4.2.4. Предотвращение несанкционированного доступа к информационным ресурсам и системам, в том числе из сети Интернет.

4.2.5. Предотвращение внедрения в информационные системы программ-вирусов и иного вредоносного программного кода.

4.2.6. Разграничение доступа пользователей к информационным ресурсам АС различного уровня и назначения.

4.2.7. Внедрение процессов минимизации полномочий и разделения обязанностей.

4.2.8. Реализация разрешительной системы доступа пользователей к работам, документам и информации ограниченного доступа.

4.2.9. Криптографическое преобразование информации, передаваемой по каналам связи.

4.2.10. Моделирование целевых атак для оценки возможности реализации недопустимых событий, в том числе для оценки практической возможности использования злоумышленниками уязвимостей критически важных средств защиты информации и программного обеспечения.

4.2.11. Аудит состояния информационной безопасности информационных систем, в том числе с привлечением сторонних организаций.

4.2.12. Мониторинг событий ИБ, обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты.

4.2.13. Проведение практических учений по противодействию компьютерным атакам.

4.2.14. Контроль почтового обмена как внутри организации, так и с внешними адресатами, в том числе защита от спама.

4.2.15. Контроль выполнения иных требований по информационной безопасности.

V. Основные локальные документы по ИБ

5.1. Для достижения целей Политики в АО «ОСК» разрабатываются и поддерживаются в актуальном состоянии следующие основные локальные документы по вопросам ИБ:

планы мероприятий по ИБ;

Руководство по защите информации от иностранных технических разведок и от ее утечки по техническим каналам (для объектов защиты, участвующих в обработке информации, составляющей государственную тайну);

Руководство по защите информации, не содержащей сведения, составляющие государственную тайну (ОСК.СМК 00.012);

документы по организации защиты информации, содержащей сведения, составляющие служебную тайну;

модели угроз информационных систем;

Положение об обработке и защите персональных данных;

Положение о коммерческой тайне;

Перечень сведений, составляющих коммерческую тайну;

инструкции по использованию средств защиты информации;

документы по обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации, владельцем которых является Общество.

5.2. Для соблюдения требований информационной безопасности при обработке информации в информационной инфраструктуре АО «ОСК» разрабатываются локальные документы, регламентирующие порядок и правила:

создания, управления учетными данными и предоставления прав доступа к информационным ресурсам, а также привилегированного доступа;

организации парольной защиты;

безопасной работы пользователей в ИС;

организации антивирусной защиты;

организации системного администрирования и администрирования ИБ;

использования корпоративной электронной почты;

безопасного взаимодействия с сетью Интернет;

обмена информацией со сторонними организациями;

осуществления удаленной работы с информационными ресурсами ИС;

подключения к другим информационным системам и сетям передачи данных (в том числе подрядчиков и иных сторонних организаций);

резервного копирования и восстановления информационных ресурсов;

обращения с машинными носителями информации ограниченного доступа;

предоставления доступа к беспроводным сетям Wi-Fi;

осуществления мониторинга и контроля состояния ИБ, обнаружения, предупреждения и ликвидации последствий компьютерных атак;

реагирования на инциденты информационной безопасности;

взаимодействия с ФСТЭК России и ФСБ России (Национальным координационным центром по компьютерным инцидентам и Лицензионным подразделением).

5.3. Локальные документы Общества по вопросам ИБ подлежат согласованию с заместителем генерального директора по безопасности и утверждению генеральным директором АО «ОСК».

VI. Контроль и ответственность

Контроль состояния информационной безопасности в Обществе осуществляется следующим образом:

6.1. Работники контролируют текущее состояние ИБ на своих рабочих местах.

6.2. Руководители структурных подразделений контролируют соблюдение подчиненными работниками требований ИБ.

6.3. Администраторы информационных систем, сетевые администраторы, администраторы ИБ и владельцы информационных ресурсов контролируют состояние закрепленных за ними ресурсов.

6.4. Отдел информационной безопасности Департамента безопасности осуществляет проверки соблюдения требований ИБ в структурных подразделениях и ИС.

Для проведения контроля могут привлекаться работники Департамента цифровой трансформации и информационных технологий, сторонние организации, имеющие необходимые лицензии на деятельность в области защиты информации, а также использоваться средства мониторинга и контроля защищенности информации.

6.5. Служебные расследования и устранение выявленных нарушений проводятся под контролем Департамента безопасности.

6.6. К работникам Общества, допустившим нарушения требований информационной безопасности, могут применяться меры воздействия в соответствии с действующим законодательством и локальными документами.

6.7. Общий контроль за выполнением требований настоящей Политики возлагается на Департамент безопасности.

VII. Заключительные положения

7.1. В Политике сформулированы базовые подходы и правила ИБ применительно к особенностям осуществления АО «ОСК» основных видов деятельности, на которые необходимо ориентироваться при организации работ по обеспечению безопасности информации и разработке локальных документов.

7.2. Политика вступает в силу с момента ее утверждения.

VIII. Порядок внесения изменений и контроль версий

8.1. Политика подлежит пересмотру по мере необходимости. Организация работ по актуализации Политики возлагается на отдел информационной безопасности Департамента безопасности АО «ОСК».

Приложение
к Политике информационной
безопасности АО «ОСК»

Модель зрелости управления информационной безопасностью

(в соответствии с международным стандартом COBIT)

Модель зрелости управления информационной безопасностью основывается на модели зрелости, определенной международным стандартом COBIT, которая определяет шесть уровней зрелости организации – с нулевого по пятый.

Нулевой уровень («несуществующий») характеризует полное отсутствие каких-либо процессов управления ИБ в рамках деятельности организации. Организация не осознает существования проблем ИБ.

Первый уровень («начальный») характеризует наличие документально зафиксированных свидетельств осознания организацией существования проблем обеспечения ИБ. Однако используемые процессы управления ИБ не стандартизованы, применяются эпизодически и бессистемно. Общий подход к управлению ИБ не выработан.

Второй уровень («повторяемый») характеризует проработанность процессов управления ИБ до уровня, когда их выполнение обеспечивается различными людьми, решающими одну и ту же задачу. Однако отсутствуют регулярное обучение и тренировки по стандартным процедурам, а ответственность возложена на исполнителя. Руководство организации в значительной степени полагается на знания исполнителей, что влечет за собой высокую вероятность возможных ошибок.

Третий уровень («определенный») характеризует то, что процессы стандартизованы, документированы и доведены до персонала посредством обучения. Однако порядок использования данных процессов оставлен на усмотрение самого персонала. Это влечет вероятность отклонений от стандартных процедур, которые могут быть не выявлены. Применяемые процедуры не оптимальны и недостаточно современны, но являются отражением практики, используемой в организации.

Четвертый уровень («управляемый») характеризует то, что обеспечиваются мониторинг и оценка соответствия используемых в организации процессов. При выявлении низкой эффективности реализуемых процессов управления ИБ обеспечивается их оптимизация. Процессы управления ИБ находятся в стадии

непрерывного совершенствования и основываются на хорошей практике. Средства автоматизации управления ИБ используются частично и в ограниченном объеме.

Пятый уровень («оптимизированный») характеризует проработанность процессов управления ИБ до уровня лучшей практики, основанной на результатах непрерывного совершенствования и сравнения уровня зрелости относительно других организаций. Защитные меры в организации используются комплексно, обеспечивая основу совершенствования процессов управления ИБ. Организация способна к быстрой адаптации при изменениях в окружении и бизнесе.