УТВЕРЖДАЮ

Генеральный директор
ООО «Сатурн»

Соколов А.А.

«___» _____ 2018 г.

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОБЩИЕ ТРЕБОВАНИЯ

[СМИБ-100]

2018г.

Оглавление

1. Общие положения

1.1. Для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ в Компании необходимо реализовать ряд процессов СМИБ, сгруппированных в виде циклической модели Деминга: «… — планирование — реализация — проверка — совершенствование — планирование — …».

1.2. Целью выполнения деятельности в рамках группы процессов «планирование» является запуск «цикла» СМИБ путем определения первоначальных планов построения, ввода в действие и контроля СОИБ, а также определения планов по совершенствованию СОИБ на основании решений, принятых на этапе «совершенствование». Выполнение деятельности на стадии «планирование» заключается в определении/корректировке области действия СОИБ, формализации подхода к оценке рисков ИБ и распределении ресурсов, проведении оценки рисков ИБ и определении/коррекции планов их обработки. Важно, чтобы все решения по реализации/корректировке СОИБ были приняты руководством Компании (далее — руководство).

1.3. Этап «реализация» выполняется по результатам выполнения этапов «планирование» и (или) «совершенствование» и заключается в выполнении всех планов, связанных с построением, вводом в действие и совершенствованием СОИБ, определенных на этапе «планирование», и (или) реализации решений, определенных на этапе «совершенствование» и не требующих выполнения деятельности по планированию соответствующих улучшений. В том числе важным является выполнение таких видов деятельности, как организация обучения и повышение осведомленности в области ИБ, реализация обнаружения и реагирования на инциденты ИБ, обеспечение непрерывности бизнеса Компании.

Компания должна выбирать защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от реализации угроз.

Компания должна применять только те защитные меры, правильность работы которых может быть проверена, при этом Компания должна регулярно оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на бизнес-цели Компании.

1.4. Целью выполнения деятельности в рамках группы процессов «проверка» является обеспечение достаточной уверенности в том, что СОИБ, включая защитные меры, функционирует надлежащим образом и адекватна существующим угрозам ИБ, а также внутренним и (или) внешним условиям функционирования Компании, связанным с ИБ. Кроме того, необходимо рассмотреть любые изменения в допущениях или в области оценки рисков.

Указанная деятельность может проводиться в любое время и с любой частотой, в зависимости от того, что является подходящим для конкретной ситуации. На этапе «проверка» необходимо осуществлять мониторинг и контроль используемых защитных мер, периодически выполнять деятельность по самооценке соответствия ИБ Компании требованиям (далее — самооценка ИБ) и проводить аудит ИБ, анализировать функционирование СОИБ в целом, в том числе со стороны руководства.

Компания должна своевременно обнаруживать проблемы, прямо или косвенно относящиеся к ИБ, потенциально способные повлиять на ее бизнес-цели. Рекомендуется выявлять причинно-следственную связь возможных проблем и строить на этой основе прогноз их развития.

Результат выполнения деятельности на этапе «проверка» является основой для выполнения деятельности по совершенствованию СОИБ.

1.5. Группа процессов «совершенствование» включает в себя деятельность по принятию

решений о реализации тактических и (или) стратегических улучшений СОИБ. Указанная деятельность, т.е. переход к этапу «совершенствование», реализуется только тогда, когда выполнение процессов этапа «проверка» дало результат, требующий совершенствования СОИБ.

При этом сама деятельность по совершенствованию СОИБ должна реализовываться в рамках групп процессов «реализация» и при необходимости — «планирование». Пример первой ситуации — введение в действие существующего плана обеспечения непрерывности бизнеса, поскольку на стадии «проверка» определена необходимость в этом. Пример второй ситуации — идентификация новой угрозы и последующие обновления оценки рисков на стадии «планирование». При этом важно, чтобы все заинтересованные стороны немедленно извещались о проводимых улучшениях СОИБ и при необходимости проводилось соответствующее обучение.

Компания должна накапливать, обобщать и использовать как свой опыт, так и опыт других организаций на всех уровнях принятия решений и их исполнения.

1.6. Для успешного функционирования СМИБ в Компании следует выполнить следующие группы требований:

- требования к организации и функционированию службы ИБ Компании;
- требования к определению/коррекции области действия СОИБ;
- требования к выбору/коррекции подхода к оценке рисков нарушения ИБ и проведению оценки рисков нарушения ИБ;
- требования к разработке планов обработки рисков нарушения ИБ;
- требования к разработке/коррекции внутренних документов, регламентирующих деятельность в области обеспечения ИБ;
- требования к принятию руководством Компании решений о реализации и эксплуатации СОИБ;
- требования к организации реализации планов обработки рисков нарушения ИБ;
- требования к разработке и организации реализации программ по обучению и повышению осведомленности в области ИБ;
- требования к организации обнаружения и реагирования на инциденты безопасности;
- требования к организации обеспечения непрерывности бизнеса и его восстановления после прерываний;
- требования к мониторингу и контролю защитных мер;
- требования к проведению самооценки ИБ;
- требования к проведению аудита ИБ;
- требования к анализу функционирования СОИБ;
- требования к анализу СОИБ со стороны руководства Компании;
- требования к принятию решений по тактическим улучшениям СОИБ;
- требования к принятию решений по стратегическим улучшениям СОИБ.

2. Требования к организации и функционированию службы информационной безопасности Компании

2.1. Для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ руководству следует сформировать службу ИБ (назначить уполномоченное лицо), а также утвердить цели и задачи ее деятельности.

Служба ИБ должна иметь утвержденные руководством полномочия и ресурсы, необходимые для выполнения установленных целей и задач, а также назначенного из числа руководства куратора. При этом служба ИБ и служба информатизации (автоматизации) не должны иметь общего куратора.

Рекомендуется наделить службу ИБ собственным бюджетом.

Компаниям, имеющим сеть филиалов или региональных представительств, рекомендуется выделять соответствующие подразделения ИБ (уполномоченных лиц) на местах, обеспечив их необходимыми ресурсами и нормативной базой.

2.2. Служба ИБ (уполномоченное лицо) должна быть наделена следующими минимальными полномочиями:

- организовывать составление и контролировать выполнение всех планов по обеспечению ИБ Компании;
- разрабатывать и вносить предложения по изменению требований и политик ИБ Компании;
- организовывать изменение существующих и принятие руководством новых внутренних документов, регламентирующих деятельность по обеспечению ИБ Компании;
- определять требования к мерам обеспечения ИБ Компании;
- контролировать работников Компании в части выполнения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь работников, имеющих максимальные полномочия по доступу к защищаемым информационным активам;
- осуществлять мониторинг событий, связанных с обеспечением ИБ;
- участвовать в расследовании событий, связанных с инцидентами ИБ, и в случае необходимости выходить с предложениями по применению санкций в отношении лиц, осуществивших НСД, например, нарушивших требования инструкций, руководств и т.п. по обеспечению ИБ Компании;
- участвовать в действиях по восстановлению работоспособности ИС после сбоев и аварий;
- участвовать в создании, поддержании, эксплуатации и совершенствовании СОИБ.

3. Требования к определению/коррекции области действия СОИБ

3.1. Должна быть документально определена/скорректирована опись структурированных по классам защищаемых информационных активов (типов информационных активов — типов информации). Классификацию информационных активов рекомендуется проводить на основании оценок ценности информационных активов для интересов (целей) Компании, например, в соответствии с тяжестью последствий потери свойств ИБ информационных активов.

3.2. В случае наличия в Компании классификации информационных активов опись информационных активов должна содержать информацию о принадлежности конкретного информационного актива к выделенным типам информационных активов.

3.3. Опись информационных активов (типов информационных активов) должна содержать перечень их объектов среды. Перечень объектов среды должен покрывать все уровни информационной инфраструктуры Компании.

3.4. Должны быть документально определены процедуры анализа и пересмотра области действия СОИБ, в частности, процедуры пересмотра при изменении перечня информационных активов Компании (типов информационных активов).

3.5. Должны быть документально определены роли по определению/коррекции области действия СОИБ, по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ. Должны быть назначены ответственные за выполнение указанных ролей.

4. Требования к выбору/коррекции подхода к оценке рисков нарушения информационной безопасности и проведению оценки рисков

4.1. Должна быть принята/корректироваться методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ.

4.2. Должны быть определены критерии принятия рисков нарушения ИБ и уровень допустимого риска нарушения ИБ.

4.3. Методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ Компании должна определять способ и порядок качественного или количественного оценивания риска нарушения ИБ на основании оценивания:

- степени возможности реализации угроз ИБ, выявленными и (или) предполагаемыми источниками угроз ИБ, зафиксированными в моделях угроз и нарушителя в результате их воздействия на объекты среды информационных активов Компании (типов информационных активов);
- степени тяжести последствий от потери свойств ИБ, в частности, свойств доступности, целостности и конфиденциальности, для рассматриваемых информационных активов (типов информационных активов).

Порядок оценки рисков нарушения ИБ должен определять необходимые процедуры оценки рисков нарушения ИБ, а также последовательность их выполнения.

4.4. Оценка рисков нарушения ИБ проводится для свойств ИБ всех информационных активов (типов информационных активов) области действия СОИБ.

4.5. В Компании рекомендуется создать и поддерживать в актуальном состоянии единый информационный ресурс (базу данных), содержащий информацию об инцидентах ИБ.

4.6. Полученные в результате оценивания рисков нарушения ИБ величины рисков должны быть соотнесены с уровнем допустимого риска, принятого в Компании. Результатом выполнения указанной процедуры является документально оформленный перечень недопустимых рисков нарушения ИБ.

4.7. Должны быть документально определены роли, связанные с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке рисков нарушения ИБ и назначены ответственные за выполнение указанных ролей.

4.8. Должны быть документально определены роли по оценке рисков нарушения ИБ и назначены ответственные за выполнение указанных ролей.

5. Требования к разработке планов обработки рисков нарушения информационной безопасности

5.1. По каждому из рисков нарушения ИБ, который является недопустимым, должен быть документально определен план, определяющий один из возможных способов его обработки:

- перенос риска на сторонние организации (например, путем страхования, указанного риска);
- уход от риска (например, путем отказа от деятельности, выполнение которой приводит к появлению риска);
- осознанное принятие риска;
- формирование требований по обеспечению ИБ, снижающих риск нарушения ИБ до допустимого уровня, и формирования планов по их реализации.

5.2. Планы обработки рисков нарушения ИБ должны быть согласованы с руководителем службы ИБ либо лицом, отвечающим в Компании за обеспечение ИБ, и утверждены руководством.

5.3. Планы реализаций требований по обеспечению ИБ должны содержать последовательность и сроки реализации и внедрения организационных, технических и иных защитных мер.

5.4. Должны быть документально определены роли по разработке планов обработки рисков нарушения ИБ и назначены ответственные за выполнение указанных ролей.

6. Требования к разработке/коррекции внутренних документов, регламентирующих СОИБ

6.1. Разработку/коррекцию внутренних документов, регламентирующих деятельность в области обеспечения ИБ в Компании, рекомендуется проводить с учетом рекомендаций по стандартизации.

6.2. Должны разрабатываться/корректироваться следующие внутренние документы:

- политика ИБ Компании;
- частные политики/требования ИБ Компании;
- документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ Компании.

Кроме того, должны быть определены перечень и формы документов, являющихся свидетельством выполнения деятельности по обеспечению ИБ в Компании.

Политика ИБ Компании должна быть утверждена руководством.

6.3. В политике (в частных политиках) ИБ должны определяться/корректироваться:

- цели и задачи обеспечения ИБ;
- основные области обеспечения ИБ;
- типы основных защищаемых информационных активов;
- модели угроз и нарушителей;
- совокупность правил, требований и руководящих принципов в области ИБ;
- основные требования по обеспечению ИБ;
- принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов;
- основные принципы повышения уровня осознания и осведомленности в области ИБ;
- принципы реализации и контроля выполнения требований политики ИБ.

6.4. Разработка/корректировка внутренних документов, регламентирующих деятельность в области обеспечения ИБ, должна проводиться на основе:

- законодательства Российской Федерации;
- нормативных актов и предписаний регулирующих и надзорных органов;
- договорных требований Компании со сторонними организациями;
- результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов).

6.5. Совокупность внутренних документов, регламентирующих деятельность в области обеспечения ИБ, должна содержать требования по обеспечению ИБ всех выявленных информационных активов (типов информационных активов), находящихся в области действия СОИБ Компании.

6.6. Документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ, должны детализировать положения политики (частных политик) ИБ и не противоречить им.

6.7. В случае наличия в структурных подразделениях Компании работников, ответственных за обеспечение ИБ, в Компании должен быть утвержден руководством порядок взаимодействия (координирования работы) службы ИБ с указанными работниками.

6.8. В составе внутренних документов, регламентирующих деятельность в области обеспечения ИБ, необходимо определить:

- перечень свидетельств выполнения деятельности;
- ответственность работников Компании за выполнение этой деятельности.

6.9. Должны быть документально определены процедуры выделения и распределения ролей в области обеспечения ИБ.

6.10. Должен быть документально определен порядок разработки, поддержки, пересмотра и контроля исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ в Компании.

6.11. Должны быть документально определены роли по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ, а также назначены ответственные за выполнение указанных ролей.

7. Требования к принятию руководством Компании решений о реализации и эксплуатации СОИБ

7.1. Решения о реализации и эксплуатации СОИБ должны утверждаться руководством Компании. В частности, в Компании требуется документально оформить решения руководства:

- об анализе и принятии остаточных рисков нарушения ИБ;
- о планировании этапов внедрения СОИБ, в частности, требований СОИБ;
- о распределении ролей в области обеспечения ИБ Компании;
- о принятии со стороны руководства планов внедрения защитных мер, направленных на реализацию требований СОИБ, СМИБ и снижение рисков ИБ;
- о выделении ресурсов, необходимых для реализации и эксплуатации СОИБ.

7.2. Все планы внедрения СОИБ, в частности, планы реализации требований СМИБ, СОИБ, планы обработки рисков нарушения ИБ и внедрения защитных мер должны быть утверждены руководством. Указанные планы должны документально фиксировать:

- последовательность выполнения мероприятий в рамках указанных планов;
- сроки начала и окончания запланированных мероприятий;
- должностных лиц (подразделения), ответственных за выполнение каждого указанного мероприятия.

7.3. Должен быть документально определен порядок разработки, пересмотра и контроля исполнения планов по обеспечению ИБ Компании.

7.4. Должны быть документально оформлены решения руководства, связанные с назначением и распределением ролей для всех структурных подразделений в соответствии с положениями внутренних документов, регламентирующих деятельность по обеспечению ИБ Компании.

8. Требования к организации реализации планов внедрения СОИБ

8.1. Должны быть документально определены и выполняться проектирование/приобретение/развертывание, внедрение, эксплуатация, контроль и сопровождение эксплуатации защитных мер, предусмотренных планами реализаций требований по обеспечению ИБ.

8.2. Для построения элементов СОИБ применительно к конкретной области или сфере деятельности Компании должны быть реализованы конкретные защитные меры, применяемые к объектам среды в соответствии с существующими в Компании требованиями по обеспечению ИБ, сформулированными в политике ИБ, концепции ИБ и других внутренних документах Компании.

8.3. Должны быть документально определены роли, связанные с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер, и назначены ответственные за выполнение указанных ролей.

9. Требования к разработке и организации реализации программ по обучению и повышению осведомленности в области информационной безопасности

9.1. Должна быть организована документально оформленная и утвержденная руководством работа с персоналом Компании в направлении повышения осведомленности и обучения в области ИБ, включая разработку и реализацию планов и программ обучения, и повышения осведомленности в области ИБ и контроля результатов выполнения указанных планов.

9.2. В планах обучения и повышения осведомленности должны быть установлены требования к периодичности обучения и повышения осведомленности.

9.3. Программы обучения и повышения осведомленности должны включать информацию:

- по существующим политикам ИБ;
- по применяемым в Компании защитным мерам;
- по правильному использованию защитных мер в соответствии с внутренними документами Компании;
- о значимости и важности деятельности работников для обеспечения ИБ.

9.4. Должен быть определен перечень документов, являющихся свидетельством выполнения программ обучения и повышения осведомленности в области ИБ. В частности, такими документами могут являться:

- документы (журналы), подтверждающие прохождение руководителями и работниками Компании обучения в области ИБ с указанием уровня образования, навыков, опыта и квалификации обучаемых;
- документы, содержащие результаты проверок обучения работников Компании;
- документы, содержащие результаты проверок осведомленности в области ИБ.

9.5. Для работника, получившего новую роль, должно быть организовано обучение или инструктаж в области ИБ, соответствующее полученной роли.

9.6. Должны быть документально определены роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю результатов, а также назначены ответственные за выполнение указанных ролей.

10. Требования к организации обнаружения и реагирования на инциденты информационной безопасности

10.1. В компании должна быть создана постоянно действующая комиссия по ИБ

10.2. Должны быть документы, регламентирующие процедуры обработки инцидентов, включающие:

- процедуры обнаружения инцидентов ИБ;
- процедуры информирования об инцидентах;
- процедуры классификации инцидентов и оценки ущерба, нанесенного инцидентом ИБ;
- процедуры реагирования на инцидент;
- процедуры анализа причин инцидентов ИБ и оценки результатов реагирования на инциденты ИБ (при необходимости с участием внешних экспертов в области ИБ).

10.3. В Компании рекомендуется сформировать и поддерживать в актуальном состоянии централизованную базу данных инцидентов ИБ. Должны быть документально определены процедуры по хранению информации об инцидентах ИБ, практиках анализа инцидентов ИБ и результатах реагирования на инциденты ИБ.

10.4. Должны быть документально определены порядки действий работников Компании при обнаружении нетипичных событий, связанных с ИБ, и информировании о данных событиях. Работники организации должны быть осведомлены об указанных порядках.

10.5. Процедуры расследования инцидентов ИБ должны учитывать действующее законодательство Российской Федерации.

10.6. Должны приниматься и выполняться документально оформленные решения по всем выявленным инцидентам ИБ.

10.7. Должны быть документально определены роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ и назначены ответственные за выполнение указанных ролей.

11. Требования к организации обеспечения непрерывности бизнеса и его восстановления после прерываний

11.1. В описи защищаемых информационных активов должны быть выделены информационные активы, существенные для обеспечения непрерывности бизнеса Компании.

11.2. Должны быть документально определены требования по обеспечению ИБ, регламентирующие вопросы обеспечения непрерывности бизнеса и его восстановления после прерывания.

11.3. Должен быть документально определен план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания. План должен содержать инструкции и порядок действий работников Компании по восстановлению бизнеса. В частности, в состав плана должны быть включены:

- условия активизации плана;
- действия, которые должны быть предприняты после инцидента ИБ;
- процедуры восстановления;
- процедуры тестирования и проверки плана;
- план обучения и повышения осведомленности работников Компании;
- обязанности работников Компании с указанием ответственных за выполнение каждого из положений плана.

11.4. Разработка планов обеспечения непрерывности бизнеса и его восстановления после прерывания должна основываться на документально оформленных результатах оценки рисков нарушения ИБ Компании применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания.

11.5. Должны быть документально определены, реализованы и использоваться защитные меры обеспечения непрерывности бизнеса применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания.

Реализация и использование защитных мер обеспечения непрерывности бизнеса и его восстановления после прерывания должны основываться на соответствующих требованиях по обеспечению ИБ.

11.6. План обеспечения непрерывности бизнеса и его восстановления после прерывания должен быть согласован с существующими в Компании процедурами обработки инцидентов ИБ.

11.7. Должно быть документально определено и выполняться периодическое тестирование плана обеспечения непрерывности бизнеса и его восстановления после прерывания. По результатам тестирования при необходимости проводится соответствующая корректировка плана. Сценарий тестирования должен быть составлен с учетом существующей в Компании модели угроз и нарушителей, а также результатов оценки рисков.

11.8. Должна быть реализована программа обучения и повышения осведомленности работников в области обеспечения непрерывности бизнеса и его восстановления после прерываний.

11.9. Должны быть документально определены и выполняться процедуры регулярного пересмотра и обновления плана обеспечения непрерывности бизнеса и его восстановления после прерывания для обеспечения уверенности в их эффективности. Процедуры пересмотра и обновления плана должны учитывать изменения в приоритетах, целях и интересах бизнеса Компании; пересмотр моделей угроз; оценку рисков нарушения ИБ.

11.10. Должны быть документально определены роли по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания и назначены ответственные за выполнение указанных ролей.

12. Требования к мониторингу и контролю защитных мер

12.1. Должны быть документально определены процедуры мониторинга СОИБ и контроля защитных мер, включая контроль параметров конфигурации и настроек средств и механизмов защиты. Указанные процедуры должны проводиться персоналом Компании, ответственным за обеспечение ИБ, и охватывать все реализованные и эксплуатируемые защитные меры, входящие в СОИБ.

12.2. Результаты выполнения процедур мониторинга СОИБ и контроля защитных мер должны документально фиксироваться.

12.3. Должны быть документально определены и выполняться процедуры сбора и хранения информации о действиях работников Компании, событиях и параметрах, имеющих отношение к функционированию защитных мер.

12.4. Информация обо всех инцидентах, выявленных в процессе мониторинга СОИБ и контроля защитных мер, должна включаться в базу данных инцидентов ИБ.

12.5. Процедуры мониторинга СОИБ и контроля защитных мер должны подвергаться

регулярным и документально зафиксированным пересмотрам в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также на основе данных об инцидентах ИБ. Порядок выполнения процедур пересмотра должен быть документально определен.

12.6. Должны быть документально определены роли, связанные с выполнением процедур мониторинга СОИБ и контроля защитных мер, а также пересмотром указанных процедур, и назначены ответственные за выполнение указанных ролей.

13. Требования к проведению самооценки информационной безопасности

13.1. Самооценка ИБ должна проводиться с установленной периодичностью.

13.2. Должна быть документально определена и реализована программа самооценок ИБ, содержащая информацию, необходимую для планирования и организации самооценок ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ в заданные сроки.

13.3. Должны быть документально определены:

- порядок формирования, сбора и хранения свидетельств самооценки ИБ;
- периодичность проведения самооценки ИБ;
- порядок хранения и использования результатов самооценки ИБ.

13.4. Для каждой проводимой в Компании самооценки ИБ необходимо документально оформить план проведения самооценки, определяющий:

- цель самооценки ИБ;
- объекты и деятельность, подвергающиеся самооценке ИБ;
- порядок и сроки выполнения мероприятий самооценки ИБ;
- распределение ролей среди работников Компании, связанных с проведением самооценки ИБ.

13.5. По результатам проведения самооценок ИБ должны быть подготовлены отчеты. Результаты самооценок ИБ, а также соответствующие отчеты должны быть доведены до руководства Компании.

13.6. Должны быть документально определены роли, связанные с выполнением программы самооценок ИБ, и назначены ответственные за выполнение указанных ролей.

14. Требования к проведению аудита информационной безопасности

14.1. Должна быть документально определена и реализовываться программа аудитов ИБ, содержащая информацию, необходимую для планирования и организации аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки.

14.2. Для каждого проводимого в Компании аудита ИБ необходимо документально оформить план аудита, определяющий:

- цель аудита ИБ;
- критерии аудита ИБ;
- область аудита ИБ;
- дату и продолжительность проведения аудита ИБ;
- состав аудиторской группы;
- описание деятельности и мероприятий по проведению аудита;

- распределение ресурсов при проведении аудита.

14.3. Должны быть оформлены договоры с аудиторскими организациями, а также документально определены:

- порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудита ИБ;
- порядок взаимодействия с аудиторской организацией в процессе проведения аудита ИБ;
- порядок взаимодействия аудиторской группы и руководства, позволяющий представителям аудиторской группы при необходимости непосредственно обращаться к руководству;
- порядок организации опроса работников;
- порядок организации наблюдения за деятельностью работников Компании со стороны представителей аудиторской организации.

14.4. По результатам проведения аудита должны быть подготовлены отчеты. Результаты аудитов, а также соответствующие отчеты должны быть доведены до руководства.

14.5. Должен быть документально определен порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудитов, в частности, отчетов аудитов.

14.6. Должны быть документально определены роли, связанные с организацией выполнения программ аудитов и планов отдельных аудитов, и назначены ответственные за выполнение указанных ролей.

15. Требования к анализу функционирования СОИБ

15.1. В Компании должен проводиться анализ функционирования СОИБ, использующий в том числе:

- результаты мониторинга СОИБ и контроля защитных мер;
- сведения об инцидентах ИБ;
- результаты проведения аудитов ИБ, самооценок ИБ;
- данные об угрозах, возможных нарушителях и уязвимостях ИБ;
- данные об изменениях внутри Компании, например, данные об изменениях в процессах и технологиях, реализуемых в рамках основного процессного потока, изменениях во внутренних документах Компании;
- данные об изменениях вне Компании, например, данные об изменениях в законодательстве Российской Федерации, изменениях в договорных обязательствах Компании.

15.2. Анализ функционирования СОИБ должен включать в том числе:

- анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению ИБ в Компании, требованиям законодательства Российской Федерации, контрактным требованиям Компании;
- анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению ИБ в Компании, требованиям политик ИБ Компании;
- оценку адекватности модели угроз Компании существующим угрозам ИБ;
- оценку рисков в области ИБ, включая оценку уровня остаточного и допустимого риска;

- проверку адекватности используемых защитных мер требованиям внутренних документов Компании и результатам оценки рисков;
- анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании защитных мер.

Результаты анализа функционирования СОИБ должны документироваться.

15.3. Должны быть документально определены роли, связанные с процедурами анализа функционирования СОИБ, и назначены ответственные за выполнение указанных ролей.

15.4. Должен быть утвержден перечень документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ. В частности, в указанный перечень документов должны входить:

- отчеты с результатами мониторинга СОИБ и контроля защитных мер;
- отчеты с результатами анализа функционирования СОИБ;
- отчеты с результатами аудитов ИБ;
- отчеты с результатами самооценок ИБ;
- документы, содержащие информацию о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ;
- документы, содержащие информацию о новых выявленных уязвимостях и угрозах ИБ;
- документы, содержащие информацию о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством;
- документы, содержащие информацию об изменениях, которые могли бы повлиять на организацию СОИБ, например, изменения в законодательстве Российской Федерации;
- документы, содержащие информацию по выявленным инцидентам ИБ;
- документы, подтверждающие выполнение требуемой деятельности по обеспечению ИБ, например, выполнение планов обработки рисков;
- документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания.

15.5. В Компании должен быть определен и утвержден руководством план выполнения деятельности по контролю и анализу СОИБ. В частности, указанный план должен содержать положения по проведению совещаний на уровне руководства, на которых в том числе производятся поиск и анализ проблем ИБ, влияющих на бизнес Компании.

15.6. Должны быть документально определены роли, связанные с подготовкой информации, необходимой для анализа СОИБ руководством, и назначены ответственные за выполнение указанных ролей.

16. Требования к принятию решений по тактическим улучшениям СОИБ

16.1. Для принятия решений, связанных с тактическими улучшениями СОИБ, необходимо рассмотреть среди прочего документально оформленные результаты:

- аудитов ИБ;
- самооценок ИБ;
- мониторинга СОИБ и контроля защитных мер;
- анализа функционирования СОИБ;
- обработки инцидентов ИБ;
- выявления новых угроз и уязвимостей ИБ;

- оценки рисков;
- анализа перечня защитных мер, возможных для применения;
- стратегических улучшений СОИБ;
- анализа СОИБ со стороны руководства;
- анализа успешных практик в области ИБ (собственных или других организаций).

16.2. Решения по тактическим улучшениям СОИБ должны быть документально зафиксированы и содержать либо выводы об отсутствии необходимости тактических улучшений СОИБ, либо должны быть указаны направления тактических улучшений СОИБ в виде корректирующих или превентивных действий:

- пересмотр процедур выполнения отдельных видов деятельности по обеспечению ИБ;
- пересмотр процедур эксплуатации отдельных видов защитных мер;
- пересмотр процедур обнаружения и обработки инцидентов;
- уточнение описи информационных активов;
- пересмотр программы обучения и повышения осведомленности персонала;
- пересмотр плана обеспечения непрерывности бизнеса и его восстановления после прерывания;
- пересмотр планов обработки рисков;
- вынесение санкций в отношении персонала;
- пересмотр процедур мониторинга СОИБ и контроля защитных мер;
- пересмотр программ аудитов;
- корректировка соответствующих внутренних документов, регламентирующих процедуры выполнения деятельности по обеспечению ИБ и эксплуатации защитных мер;
- ввод новых или замена используемых защитных мер.

К тактическим улучшениям СОИБ следует относить корректирующие или превентивные действия, связанные с пересмотром отдельных процедур выполнения деятельности в рамках СОИБ Компании и не требующие пересмотра политики ИБ и частных политик ИБ. Как правило, тактические улучшения СОИБ не требуют выполнения деятельности в рамках этапа «планирование» СМИБ.

К стратегическим улучшениям СОИБ следует относить корректирующие или превентивные действия, связанные с пересмотром политики ИБ и частных политик ИБ Компании, с последующим выполнением соответствующих тактических улучшений СОИБ.

Стратегические улучшения СОИБ всегда требуют выполнения деятельности в рамках этапа «планирование» СМИБ.

16.3. Вся деятельность по реализации тактических улучшений должна документально регистрироваться. Должны быть определены документы, содержащие планы реализации тактических улучшений СОИБ, и документы, в которых фиксируются результаты выполнения указанных планов.

16.4. Деятельность, связанная с реализацией тактических улучшений СОИБ, должна быть санкционирована и контролироваться руководством службы ИБ Компании.

16.5. Должны быть документально определены и выполняться процедуры согласования и информирования заинтересованных сторон о тактических улучшениях СОИБ, в частности, об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям по обеспечению ИБ, а также должны быть документально зафиксированы результаты выполнения указанных процедур.

16.6. В случаях принятия решений по тактическим улучшениям СОИБ должны быть назначены

ответственные за их реализацию.

17. Требования к принятию решений по стратегическим улучшениям СОИБ

17.1. Для принятия решений, связанных со стратегическими улучшениями СОИБ, необходимо рассмотреть среди прочего документально оформленные результаты:

- аудитов ИБ;
- самооценок ИБ;
- мониторинга СОИБ и контроля защитных мер;
- анализа функционирования СОИБ;
- обработки инцидентов ИБ;
- выявления новых информационных активов Компании или их типов;
- выявления новых угроз и уязвимостей ИБ;
- оценки рисков;
- пересмотра основных рисков ИБ;
- анализа СОИБ со стороны руководства;
- анализа успешных практик в области ИБ (собственных или других организаций);
- изменения в законодательстве Российской Федерации;
- изменения интересов, целей и задач бизнеса Компании;
- изменения контрактных обязательств Компании.

17.2. Решения по стратегическим улучшениям СОИБ должны быть документально зафиксированы и содержать либо выводы об отсутствии необходимости стратегических улучшений СОИБ, либо указывать направления стратегических улучшений СОИБ в виде корректирующих или превентивных действий:

- уточнение/пересмотр целей и задач обеспечения ИБ, определенных в рамках политики ИБ или частных политик ИБ;
- изменение в области действия СОИБ;
- уточнение описи типов информационных активов;
- пересмотр моделей угроз и нарушителей;
- изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ.

17.3. Вся деятельность по реализации стратегических улучшений должна документально регистрироваться. Должны быть определены документы, содержащие планы реализации стратегических улучшений СОИБ, и документы, в которых фиксируются результаты выполнения указанных планов.

17.4. Деятельность, связанная с реализацией стратегических улучшений СОИБ, должна быть санкционирована и контролироваться руководством Компании.

17.5. В случае стратегических улучшений СОИБ должна быть выполнена деятельность по реализации соответствующих тактических улучшений СОИБ для всех необходимых процедур обеспечения ИБ, используемых защитных мер и соответствующих внутренних документов.

17.6. В частности, необходимо выполнить:

- выработку планов тактических улучшений СОИБ;
- уточнение планов обработки рисков;
- уточнение программы внедрения защитных мер;
- уточнение процедур использования защитных мер.

17.7. Должны быть документально определены и выполняться процедуры согласования и

информирования заинтересованных сторон о стратегических улучшениях СОИБ, в частности, об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям по обеспечению ИБ, а также должны быть документально зафиксированы результаты выполнения указанных процедур.

17.8. В случаях принятия решений по стратегическим улучшениям СОИБ должны быть назначены ответственные за их реализацию.

18. История изменений

№	Дата	Версия	Предмет изменений	Автор
1.				
2.				
3.				