Автономная некоммерческая организация
дополнительного профессионального образования
«Образовательный центр Цифровой Следователь»
(АНО ДПО «ОЦЦС»)

УТВЕРЖДЕНО
Приказом Директора АНО ДПО «ОЦЦС»
№ 5 от 25 августа 2021 года

_____ Пак С. А.

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР ЦИФРОВОЙ СЛЕДОВАТЕЛЬ»

2021 г.

Оглавление

1. Термины и определения

Информационная инфраструктура – система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия. Информационная инфраструктура включает совокупность информационных центров, банков данных и знаний, систем связи; обеспечивает доступ потребителей к информационным ресурсам.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для учреждения; находящаяся в распоряжении учреждения и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Объект среды информационного актива – материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т.д.).

Система информационной безопасности – совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

Роль – заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом.

Ресурс – актив учреждения, который используется или потребляется в процессе выполнения некоторой деятельности.

Угроза – опасность, предполагающая возможность потерь (ущерба).

Риск – мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

Защитная мера – сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения ИБ.

Угроза информационной безопасности – угроза нарушения свойств ИБ: доступности, целостности или конфиденциальности информационных активов.

Злоумышленник – лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий.

Уязвимость информационной безопасности – слабое место в инфраструктуре, которое может быть использовано для реализации или способствовать реализации угрозы ИБ.

Ущерб – утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры организации или другой вред активам и (или) инфраструктуре учреждения, наступивший в результате реализации угроз ИБ через уязвимости ИБ.

Инцидент информационной безопасности – событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются:

– нарушение или возможное нарушение работы средств защиты информации в составе учреждения;

– нарушение или возможное нарушение требований законодательства РФ, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов учреждения в области обеспечения ИБ, нарушение или возможное нарушение в выполнении процессов учреждения;

– нанесение или возможное нанесение ущерба учреждению и (или) его клиентам.

Нарушитель информационной безопасности – субъект, реализующий угрозы ИБ, нарушая предоставленные ему полномочия по доступу к активам учреждения или по распоряжению ими.

Модель нарушителя информационной безопасности – описание и классификация нарушителей ИБ, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз ИБ со стороны указанных нарушителей.

Модель угроз информационной безопасности – описание актуальных для учреждения источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба.

Риск нарушения информационной безопасности – риск, связанный с угрозой ИБ.

Оценка риска нарушения информационной безопасности – систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения ИБ, связанных с использованием информационных активов учреждения на всех стадиях их жизненного цикла.

Обработка риска нарушения информационной безопасности – процесс выбора и осуществления защитных мер, снижающих риск нарушения ИБ, или мер по переносу, принятию или уходу от риска.

Остаточный риск нарушения информационной безопасности – риск, остающийся после обработки риска нарушения ИБ.

Допустимый риск нарушения информационной безопасности – риск нарушения ИБ, предполагаемый ущерб от которого учреждение в данное время и в данной ситуации готово принять.

Политика информационной безопасности – документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенная для учреждения в целом.

Частная политика информационной безопасности – документация, детализирующая положения политики ИБ применительно к одной или нескольким областям ИБ.

Мониторинг ИБ – постоянное наблюдение за объектами и субъектами, влияющими на ИБ учреждения, а также сбор, анализ и обобщение результатов наблюдений.

Оценка соответствия информационной безопасности – систематический и документируемый процесс получения свидетельств деятельности учреждения по реализации требований ИБ и установлению степени выполнения в учреждении критериев оценки (аудита) ИБ.

Аудит информационной безопасности – независимая оценка соответствия ИБ, выполняемая работниками организации, являющейся внешней по отношению к учреждению, допускающая возможность формирования профессионального аудиторского суждения о состоянии ИБ учреждения.

Самооценка информационной безопасности – оценка соответствия информационной безопасности, выполняемая работниками учреждения.

2. Обозначения и сокращения

ИБ – информационная безопасность;

Учреждение – АНО ДПО ОЦЦС

НСД – несанкционированный доступ;

НРД – нерегламентированные действия в рамках предоставленных полномочий;

СКЗИ – средство криптографической защиты информации;

СИБ – система информационной безопасности;

СОИБ – система обеспечения информационной безопасности;

ЭВМ – электронная вычислительная машина.

3. Общие положения

3.1 Политика информационной безопасности (далее – Политика) определяет цели и задачи построения системы обеспечения информационной безопасности учреждения и вместе с другими документами устанавливает системно связанную совокупность правил, требований и руководящих принципов в области обеспечения информационной безопасности (далее – ИБ).

3.2 Политика ИБ разрабатывается на основе накопленного в учреждении опыта в области обеспечения ИБ и учитывает современное состояние и ближайшие перспективы развития информационных технологий в учреждении, цели, задачи и правовые основы их эксплуатации, режимы функционирования, а также содержит анализ угроз безопасности для объектов и субъектов информационных отношений учреждения.

3.3 Политика является методологической основой для:

– формирования и проведения единой политики в области обеспечения ИБ в учреждении;

– принятия управленческих решений и разработке практических мер по воплощению политики информационной безопасности и выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ИБ;

– координации деятельности структурных подразделений учреждения при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению ИБ;

– разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения ИБ в учреждении.

3.4 Общую организацию мероприятий по обеспечению информационной безопасности и контроль за соблюдением установленных внутренними нормативными документами требований осуществляет Руководство учреждения.

3.5 Политика распространяется на все структурные подразделения учреждения и обязательна к исполнению всеми его сотрудниками и должностными лицами при использовании информационных активов учреждения. Руководители структурных подразделений учреждения ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

3.6 Соблюдение настоящей Политики является элементом корпоративной этики, в связи с чем на уровень ИБ учреждения серьезное влияние оказывают отношения, как в коллективе, так и между коллективом и Руководством учреждения. Понимая, что наиболее критичным элементом безопасности учреждения является персонал, Руководство учреждения стремится поощрять заинтересованность и осведомленность персонала в решении проблем ИБ.

3.7 Документами, детализирующими положения Политики применительно к одной или нескольким областям ИБ, видам и технологиям деятельности учреждения, являются частные политики по обеспечению ИБ (далее – Частные политики), которые оформляются как отдельные внутренние нормативные документы учреждения, разрабатываются и согласовываются в соответствии с установленным в учреждении порядком.

4. Исходная концептуальная схема (парадигма) обеспечения информационной безопасности

4.1 Сущность бизнеса заключается в вовлечении актива, принадлежащего учреждению, в бизнес-процесс. Эта деятельность всегда подвержена рискам, так как и на сам актив, и на бизнес-процесс могут воздействовать различного рода угрозы.

4.2 В основе исходной концептуальной схемы ИБ лежит противоборство собственника и злоумышленника с целью получения контроля над информационными

активами. Однако другие, незлоумышленные действия или источники угроз также лежат в сфере рассмотрения настоящей Политики.

Если злоумышленнику удается установить такой контроль, то как самому учреждению, так и клиентам, которые доверили ему свои собственные активы, наносится ущерб.

4.3 Руководство учреждения должно знать, что защищать. Для этого необходимо определить и защитить все информационные активы (ресурсы), реализация угроз в отношении которых может нанести ущерб.

4.4 Наибольшими возможностями для нанесения ущерба учреждению обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является прямое нецелевое использование предоставленного ему в порядке выполнения служебных обязанностей контроля над активами либо нерегламентированная деятельность для получения контроля над активами. При этом он будет стремиться к сокрытию следов своей деятельности.

Внешнему злоумышленнику, как правило, требуется сообщник внутри учреждения.

Незлоумышленные действия собственных работников создают либо уязвимости ИБ, либо инциденты, влияющие на свойства доступности, целостности и конфиденциальности информационного актива или параметры системы, которая этот актив поддерживает.

4.5 Практически никогда не известно о готовящемся нападении, оно, как правило, бывает неожиданным. Нападения, как правило, носят локальный и конкретный по месту, цели и времени характер.

4.6 Злоумышленник изучает объект нападения, как правило, не только теоретически, никак не проявляя себя, но и практически, путем выявления уязвимостей ИБ. Путем поиска или создания уязвимостей ИБ он отрабатывает наиболее эффективный метод нападения (получения контроля над активом).

4.7 Уязвимость ИБ создает предпосылки к реализации угрозы через нее (инцидент ИБ). Реализация угрозы нарушения ИБ приводит к утрате защищенности интересов (целей) учреждения в информационной сфере, в результате чего наносится ущерб. Тяжесть ущерба совместно с вероятностью приводящего к нему инцидента ИБ определяют величину риска.

4.8 Учреждение осуществляет свою деятельность путем реализации совокупности процессов, среди которых возможно выделение следующих групп:

– основные процессы, обеспечивающие достижение целей и задач;

– вспомогательные процессы, обеспечивающие качество, в том числе обеспечение ИБ;

– процессы менеджмента (управления), обеспечивающие поддержку параметров основных и вспомогательных процессов в заданных пределах и их корректировку в случае изменения внешних или внутренних условий.

Такое разделение процессов является условным, так как основные и вспомогательные процессы нередко образуют единое целое, например, функционирование защитных мер составляет часть группы основных процессов. В то же время процессы менеджмента отделены от основных и вспомогательных процессов, которые являются объектами менеджмента.

4.9 Совокупность защитных мер, реализующих обеспечение ИБ, и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение, составляет систему информационной безопасности (СИБ) учреждения.

Совокупность процессов менеджмента ИБ, включая ресурсное и административное (организационное) обеспечение этих процессов, составляет систему менеджмента информационной безопасности (СМИБ) учреждения.

Совокупность СИБ и СМИБ составляет систему обеспечения информационной безопасности (СОИБ).

4.10 Процессы эксплуатации защитных мер функционируют в реальном времени. Совокупность защитных мер и процессов их эксплуатации должна обеспечивать текущий требуемый уровень ИБ в условиях штатного функционирования, а также в условиях реализации угроз, учтенных в моделях учреждения и приводящих к возникновению:

– локальных инцидентов ИБ;

– широкомасштабных катастроф и аварий различной природы, последствия которых могут иметь отношение к ИБ учреждения.

4.11 СОИБ должна быть определена, спланирована и регламентирована. Однако даже правильно выстроенные процессы и используемые защитные меры в силу объективных причин со временем имеют тенденцию к ослаблению своей эффективности. Это неминуемо ведет к деградации системы защиты и возрастанию рисков нарушения ИБ.

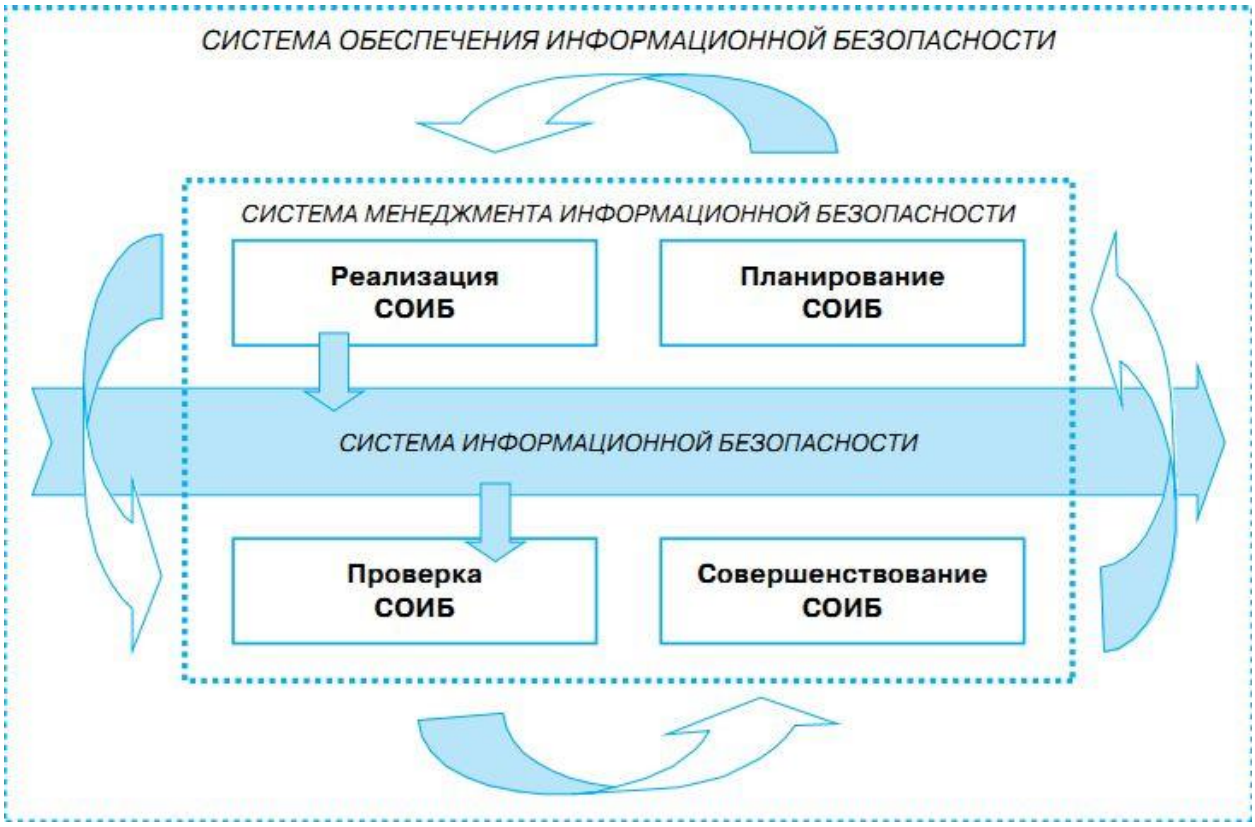
Для поддержания системы защиты на должном уровне в качестве оперативной меры используется мониторинг событий и инцидентов в СИБ. Менеджмент событий и инцидентов безопасности, полученных в результате мониторинга ИБ, позволяет избежать деградации и обеспечить требуемый уровень безопасности активов.

4.12 Стратегия обеспечения ИБ, таким образом, заключается как в эффективном использовании по имеющемуся плану заранее разработанных мер по обеспечению ИБ, противостоящих атакам злоумышленников, так и в регулярном пересмотре моделей и политик ИБ, а также корректировке СОИБ. В случае реализации угроз должен быть использован дополнительный (специально разработанный) план действий, позволяющий свести к минимуму возможные потери и восстановить СОИБ.

4.13 Основой для построения СОИБ являются требования законодательства РФ, нормативные акты учреждения, контрактные требования, а также условия ведения бизнеса, выраженные на основе идентификации активов учреждения, построения модели нарушителей и угроз.

4.14 Обеспечение безопасности информации – процесс, осуществляемый Руководством учреждения, подразделениями защиты информации и сотрудниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри учреждения, и каждый сотрудник учреждения должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности учреждения. И ее эффективность зависит от участия руководства учреждения в обеспечении информационной безопасности.

4.15 Руководству учреждения необходимо инициировать, поддерживать и контролировать выполнение процессов СОИБ. Степень выполнения указанной деятельности со стороны руководства определяется осознанием необходимости обеспечения ИБ. Осознание необходимости обеспечения ИБ проявляется в использовании Руководством учреждения бизнес-преимуществ обеспечения ИБ, способствующих формированию условий для дальнейшего развития бизнеса организации с допустимыми рисками.



4.16 Осознание необходимости обеспечения ИБ является внутренним побудительным мотивом Руководства постоянно инициировать, поддерживать, анализировать и контролировать СОИБ в отличие от ситуации, когда решение о выполнении указанных видов деятельности либо принимается в результате возникших проблем, либо определяется внешними факторами.

4.17 Осознание необходимости обеспечения ИБ учреждения выражается посредством выполнения в рамках СМИБ деятельности со стороны Руководства, направленной на инициирование, поддержание, анализ и контроль СОИБ.

5. Цели и задачи обеспечения информационной безопасности

5.1. Обеспечение информационной безопасности учреждения заключается в реализации, эксплуатации и совершенствовании совокупности защитных мер, защитных средств и процессов, включая ресурсное и административное (организационное) обеспечение, а также части менеджмента учреждения, предназначенного для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.

5.2. Основными целями обеспечения ИБ являются:

– предупреждение угроз информационной безопасности;

– снижение рисков информационной безопасности до приемлемых для учреждения уровней;

– достижение адекватности применяемых защитных мер актуальности и масштабу угроз информационной безопасности;

– предотвращение и/или снижение ущерба от реализации угроз (инцидентов) информационной безопасности, минимизация расходов на восстановление;

– соответствие требованиям законодательства, требованиям надзорных и регулирующих органов;

– обеспечение стабильности функционирования учреждения (обеспечение непрерывности его деятельности);

– повышение доверия к учреждению со стороны клиентов и контрагентов.

5.3. Для достижения перечисленных целей защиты необходимо эффективное решение следующих задач:

– разработка и совершенствование нормативной и распорядительной документации учреждения по ИБ (Политики, регламенты и положения ИБ, должностные инструкции персонала и т.п.);

– создание и поддержка организационной структуры управления информационной безопасностью, фиксирование ответственности персонала за деятельность, связанную с обеспечением ИБ;

– своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба и нарушению нормального функционирования учреждения;

– анализ информационной инфраструктуры учреждения с целью выявления и устранения уязвимостей ИБ;

– разработка, внедрение и контроль защитных мер, адекватных характеру выявленных угроз и уязвимостей, с учетом затрат на их реализацию и совместимости этих мер с действующим технологическим процессом;

– создание механизмов мониторинга событий и оперативного реагирования на инциденты информационной безопасности;

– организация мероприятий по повышению осведомленности, обучению и аттестация персонала учреждения по вопросам ИБ;

– информирование Руководства учреждения о текущем состоянии и проблемах в обеспечении информационной безопасности учреждения;

– оценка состояния ИБ защищаемых информационных активов и выявление признаков деградации используемых защитных мер.

6. Основные принципы обеспечения информационной безопасности

6.1. Построение системы, обеспечения безопасности информации учреждения, и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

– Законность предполагает осуществление защитных мероприятий и разработку системы информационной безопасности в соответствии с действующим законодательством в области информационных технологий и защиты информации. Принятые меры информационной безопасности не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях к информации конкретных подсистем.

– Системный подход к построению СОИБ предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности. Система защиты должна строиться с учетом не только всех известных путей реализации угроз безопасности, но и возможности появления принципиально новых.

– Комплексное использование методов и средств защиты информационных активов предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано и обеспечиваться техническими средствами, организационными и правовыми мерами.

– Непрерывность. Защита информации - не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех стадиях обработки защищаемой информации Деятельность по обеспечению информационной безопасности является составной частью повседневного функционирования учреждения.

– Наблюдаемость и оцениваемость обеспечения информационной безопасности заключается в том, что результаты применения защитных мер должны быть наблюдаемы и регистрируемы и впоследствии оценены службой информационной безопасности;

– Своевременность предполагает упреждающий характер мер обеспечения информационной безопасности, в том числе закладывание защитных механизмов на ранних стадиях разработки информационных систем.

– Совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, анализа функционирования информационных систем учреждения и защитных механизмов с учетом вновь выявляемых способов несанкционированного доступа к информации, изменений нормативных требований по ИБ, достигнутого отечественного и зарубежного опыта в этой области.

– Целесообразность предполагает соответствие уровня затрат на обеспечение информационной безопасности ценности информационных активов и величине возможного ущерба. Используемые меры и средства защиты информации не должны заметно ухудшать эргономические показатели работы информационных систем учреждения. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

– Персональная ответственность за нарушения требований информационной безопасности возлагается непосредственно на сотрудников, допустивших нарушения, и руководителей подразделений, где допущены нарушения. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму. Все работники должны иметь представление об ответственности за правонарушения в области информационной безопасности.

– Минимизация полномочий означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

– Исключение конфликта интересов (разделение функций) предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что ни один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования информацией и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками или подразделениями учреждения. Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции с тем, чтобы они не имели возможности скрывать совершение неправомерных

действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

– Взаимодействие и сотрудничество предполагает создание благоприятной атмосферы в коллективах структурных подразделений. В такой обстановке сотрудники должны осознанно соблюдать установленные правила. Важным элементом эффективной системы обеспечения информационной безопасности является высокая культура работы с информацией. Руководство учреждения несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, за создание корпоративной культуры, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности. Все сотрудники должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

– Гибкость системы обеспечения информационной безопасности должна заключаться в способности реагировать на изменения внешней среды и условий осуществления учреждением своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры;
- изменение существующих или внедрение принципиально новых информационных систем;
- новые технические средства;
- новые виды деятельности; новые услуги, продукты.

– Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые.

– Открытость алгоритмов и механизмов защиты состоит в том, что она не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже разработчикам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

– Простота применения средств защиты заключается в том, что механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

– Обоснованность и техническая реализуемость: объекты информационной инфраструктуры, в том числе средства защиты информации должны соответствовать современному уровню развития, установленным нормам и требованиям, а также быть обоснованы с точки зрения достижения заданного уровня информационной безопасности и экономической целесообразности.

– Специализация и профессионализм предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться

профессионально подготовленными специалистами учреждения (специалистами подразделений защиты информации).

– Контролируемость предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения информационной безопасности. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

7. Объекты защиты

7.1. В целях обеспечения информационной безопасности деятельности учреждения защите подлежат:

– информационные активы, включающие коммерческую или служебную тайну, персональные данные, платежную информацию и другие сведения, ограниченного доступа, а также любую открытую (общедоступную) информацию, необходимую для деятельности учреждения, независимо от формы и вида ее представления;

– информационная инфраструктура, включающая автоматизированные системы обработки и анализа информации; технические и программные средства вычислительной техники; средства передачи и отображения информации, в том числе каналы информационного обмена и телекоммуникационное оборудование; системы и средства защиты информации; объекты и помещения, в которых размещены компоненты информационной инфраструктуры учреждения.

7.2. Информационная инфраструктура, может быть представлена в виде иерархии следующих основных уровней:

– физического (линии связи, аппаратные средства и пр.);

– сетевого оборудования (сетевые аппаратные средства: маршрутизаторы, коммутаторы, концентраторы и пр.);

– сетевых приложений и сервисов;

– операционных систем;

– систем управления базами данных;

– бизнес-процессов.

7.3. В соответствии с иерархией уровней информационная инфраструктура учреждения представляется системой, имеющей в своем составе структурные и функциональные элементы.

7.4. Информационная инфраструктура учреждения состоит из следующих основных функциональных элементов:

– рабочих станций - отдельных ЭВМ (в т.ч. мобильных и персональных) или терминалов сети, на которых реализуются автоматизированные рабочие места пользователей (операторов, абонентов и т.д.);

– серверов или host-машин (служб печати, файлов, баз данных и т.п.) выделенных (или не выделенных, то есть совмещенных с рабочими станциями) высокопроизводительных ЭВМ, предназначенных для реализации функций хранения, печати данных, обслуживания рабочих станций сети и др. действий;

– сетевых устройств (маршрутизаторов, коммутаторов, шлюзов, центров коммутации пакетов, коммуникационных ЭВМ) - элементов, обеспечивающих соединение нескольких сетей передачи данных, либо нескольких сегментов одной и той же сети, возможно имеющих различные протоколы взаимодействия;

– средств и систем связи и передачи данных;

– средств защиты информации;

– технических средств приема, передачи и обработки информации (телефонии, звуко и видеозаписи, звукоусиления, звуко и видео воспроизведения, переговорных и телевизионных устройств, средств изготовления, тиражирования документов и других технических средств обработки речевой, графической, видео и буквенно цифровой защищаемой информации);

– каналов и линий связи (выделенных, коммутируемых, локальных и т.д.).

Все вышеуказанные функциональные элементы и созданные на их основе АС различного уровня и назначения, при условии, что они предназначены для передачи, обработки и хранения защищаемой информации, относятся к основным техническим средствам и системам (далее - ОТСС).

7.5. К вспомогательным техническим средствам и системам (далее - ВТСС), относятся технические средства и системы, не предназначенные для передачи, обработки и хранения защищаемой информации, но размещаемые совместно с ОТСС или в защищаемых помещениях.

7.6. Постоянный анализ и изучение инфраструктуры учреждения с целью выявления и устранения уязвимостей ИБ – основа эффективной работы СОИБ

8. Модели угроз и нарушителей

8.1 Модели угроз и нарушителей являются основным инструментом учреждения при развертывании, поддержании и совершенствовании СОИБ.

8.2 Модели ИБ (угроз и нарушителя) носят прогнозный характер и разрабатываются на основе фактов прошлого и опыта, но ориентированы на будущее. Чем обоснованнее и точнее сделан прогноз в отношении актуальных рисков нарушения ИБ, тем адекватнее и эффективнее будут планируемые и предпринимаемые усилия по обеспечению требуемого уровня ИБ.

8.3 При разработке моделей угроз и моделей нарушителя необходимо учитывать, что из всех возможных объектов атак с наибольшей вероятностью нарушитель выберет наиболее слабо контролируемый, где его деятельность будет оставаться необнаруженной максимально долго.

8.4 Главной целью нарушителя является нарушение характеристик безопасности защищаемых объектов путем модификации, разрушения или блокирования программных и технических средств, ознакомления с защищаемой информацией, а также навязывания ложной информации, или побуждения к принятию неверных решений.

8.5 Наиболее эффективным для нарушителя и наиболее опасным считается получение контроля над информационными активами на уровне бизнес-процессов, например путем раскрытия конфиденциальной аналитической информации. Нападения, осуществляемое через иные уровни, требуют специфических опыта, знаний и ресурсов (в т.ч. временных) и поэтому менее эффективны по соотношению «затраты / получаемый результат».

8.6 Модель нарушителя содержит описание предположений о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

8.7 Нарушитель может действовать на различных этапах жизненного цикла информационных систем (далее - ИС), обрабатывающих информационные активы учреждения, как разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств ИС.

В зависимости от возможных объектов атак выделяются:

– этапы разработки, производства, хранения, транспортировки, ввода в эксплуатацию;

– этап эксплуатации программных и технических средств;

– этап модернизации, вывода из эксплуатации программных и технических средств.

8.8 По отношению к учреждению нарушители могут быть разделены на внешних и внутренних нарушителей:

– внешних нарушителей, осуществляющих атаки вне пределов контролируемой зоны учреждения;

– внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны учреждения.

8.9 Внутренние нарушители.

В качестве потенциальных внутренних нарушителей рассматриваются:

– зарегистрированные пользователи информационных систем;

– сотрудники, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем учреждения, но имеющие доступ в здания и помещения;

– персонал, обслуживающий технические объекты информационной инфраструктуры;

– сотрудники, задействованные в разработке и сопровождении программного обеспечения;

– сотрудники, обеспечивающие безопасность;

– руководители различных уровней.

8.10 Внешние нарушители.

В качестве потенциальных внешних нарушителей рассматриваются:

– бывшие сотрудники;

– представители организаций, взаимодействующих по вопросам технического обеспечения;

– клиенты;

– посетители зданий и помещений учреждения;

– конкурирующие с учреждением организации;

– члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;

– лица, случайно или умышленно проникшие в корпоративную информационную систему учреждения из внешних телекоммуникационных сетей (хакеры).

8.11 В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

– нарушитель скрывает свои несанкционированные действия от других сотрудников учреждения;

– несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;

– в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;

– внешний нарушитель может действовать в сговоре с внутренним нарушителем.

8.12 Модель угроз применяется при решении следующих задач:

– анализа защищенности от угроз безопасности информационных активов в ходе организации и выполнения работ по обеспечению безопасности информации;

– разработки системы защиты информации, обеспечивающей нейтрализацию угроз с использованием методов и способов защиты информации;

– проведения мероприятий, направленных на предотвращение несанкционированного доступа (далее - НСД) в информационные системы и к обрабатываемым в них информационным активам, включая предотвращение несанкционированного воздействия на технические и программные средства информационных систем;

– контроля за обеспечением уровня защищенности информационных активов;

– определения совокупности условий и факторов, создающих опасность нарушения характеристик безопасности;

– определения типов источников угроз.

8.13 Разработка модели базируется на следующих принципах:

– безопасность информационных активов при их обработке в информационных системах обеспечивается с помощью системы защиты информации;

– при формировании модели угроз учитываются как угрозы, осуществление которых нарушает безопасность информационных активов (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз;

– информационные активы обрабатываются и хранятся в информационных системах с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации;

– нарушитель может действовать на различных этапах жизненного цикла информационной системы или системы защиты.

8.14 Угрозы ИБ реализуются их источниками (источниками угроз ИБ), которые могут воздействовать на объекты информационной инфраструктуры учреждения через уязвимости ИБ. В случае успешной реализации угрозы ИБ информационные активы теряют часть или все свойства ИБ.

8.15 Основными источниками угроз ИБ являются:

– неблагоприятные события природного, техногенного и социального характера;

– террористы и криминальные элементы;

– зависимость от поставщиков/провайдеров/партнеров/клиентов;

– сбои, отказы, разрушения/повреждения программных и технических средств;

– работники учреждения, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);

– работники учреждения, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками учреждения, но осуществляющие попытки НСД и НРД (внешние нарушители ИБ);

– несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

8.16 Наиболее актуальные источники угроз на физическом уровне, уровне сетевого оборудования и уровне сетевых приложений:

– внешние нарушители ИБ: лица, разрабатывающие/распространяющие вирусы и другие вредоносные программные коды; лица, организующие DoS, DDoS и иные виды атак; лица, осуществляющие попытки НСД и НРД;

– внутренние нарушители ИБ: персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, администраторы серверов, сетевых приложений и т.п.;

– комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие совместно и (или) согласованно;

– сбои, отказы, разрушения/повреждения программных и технических средств.

8.17 Наиболее актуальные источники угроз на уровнях операционных систем, систем управления базами данных:

– внутренние нарушители ИБ: администраторы ОС, администраторы СУБД, администраторы ИБ и т.д.;

– комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие в сговоре (на данных уровнях и уровне бизнес-процессов реализация угроз внешними нарушителями ИБ, действующими самостоятельно без соучастия внутренних, практически невозможна).

8.18 Следует учитывать, что со временем угрозы, их источники и риски могут изменяться, поэтому модели должны периодически пересматриваться.

8.19 Реализация угрозы нарушения ИБ приводит к утрате защищенности интересов (целей) учреждения в информационной сфере, в результате чего учреждению наносится ущерб. Тяжесть ущерба совместно с вероятностью приводящего к нему инцидента ИБ определяют величину риска.

9. Менеджмент документации по информационной безопасности

9.1 Для обеспечения согласованности, целенаправленности, планомерности деятельности по обеспечению ИБ эта деятельность должна быть документирована.

9.2 Документы по обеспечению ИБ позволяют определить и довести до каждого работника правила и требования по обеспечению ИБ, которыми он должен руководствоваться в своей производственной деятельности, а также определить порядок контроля за их соблюдением.

9.3 Деятельность по обеспечению ИБ осуществляется на основе следующих документов:

– действующих законодательных актов и нормативных документов Российской Федерации по обеспечению ИБ;

– внутренних нормативных документов учреждения по обеспечению ИБ.

9.4 В состав внутренних нормативных документов учреждения по обеспечению ИБ включаются следующие виды документов (документированной информации), организованных в виде приведенной на рисунке иерархической структуры:

– документы первого уровня: документы, содержащие положения корпоративной политики ИБ, определяют высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенные для учреждения в целом;

– документы второго уровня: документы, содержащие положения частных политик, детализируют положения корпоративной политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности учреждения;

– документы третьего уровня: документы, содержащие положения ИБ, применяемые к процедурам (порядку выполнения действий или операций) обеспечения ИБ, содержат правила и параметры, устанавливающие способ осуществления и выполнения конкретных действий, связанных с ИБ, в рамках технологических процессов, используемых в учреждении, либо ограничения по выполнению отдельных действий, связанных с реализацией защитных мер, в используемых технологических процессах (технические задания, регламенты, порядки, инструкции);

– документы четвертого уровня: документы, содержащие свидетельства выполненной деятельности по обеспечению ИБ, отражают достигнутые результаты (промежуточные и окончательные), относящиеся к обеспечению ИБ.

9.5 Документы первого уровня (корпоративная политика) определяют на высоком (общем) уровне цели и задачи обеспечения ИБ, включая способы контроля реализации требований политики ИБ учреждения, а также содержание, назначение и требования к деятельности по обеспечению ИБ без указания специфических деталей. Здесь рекомендуется определять высокоуровневые правила и требования к деятельности по управлению рисками, в том числе по анализу и выработке позиций в отношении рисков.

9.6 Второй уровень документов (частные политики) по обеспечению ИБ составляют документы, определяющие правила, требования и принципы, используемые применительно к отдельным областям ИБ, видам и технологиям деятельности учреждения. Кроме того, в состав документов данного уровня рекомендуется включить планы работ по обеспечению ИБ.

9.7 Документы второго уровня формируются на основании принципов, требований и задач, определенных в документах первого уровня, с учетом детализации, уточнения и дополнительной классификации активов и угроз, определения владельцев активов, анализа, оценки рисков и возможных последствий реализаций угроз в границах области действия регламентируемой области или технологии.

9.8 Третий уровень документов по обеспечению ИБ составляют документы, содержащие требования к процедурам обеспечения ИБ, выполняемым работниками в рамках технологических процессов, реализующих технологии, требования ИБ, к которым определены в документах второго уровня. К таким документам, относятся, например:

– инструкции по обеспечению ИБ, в том числе и должностные;

– руководства по обеспечению ИБ;

– методические указания по обеспечению ИБ;

– документы, содержащие требования к конфигурациям.

Инструкции, руководства, методические указания по обеспечению ИБ содержат свод правил, устанавливающих порядок и способ выполнения отдельных операций по обеспечению ИБ. К ним предъявляются повышенные требования четкости и ясности изложения текста. Документы этого уровня, в отличие от документов вышестоящего

уровня, описывают конкретные приемы и порядок действий сотрудников для решения определенных им (например, ролью) задач либо конкретные ограничения.

9.9 Четвертый уровень документов по обеспечению ИБ составляют документы, содержащие записи о результатах реализации деятельности по обеспечению ИБ, регламентированной документами верхних уровней иерархии. Свидетельства выполненной деятельности совместно с документами более высоких уровней иерархии могут служить документированным доказательством реализации требований ИБ при проведении внутреннего контроля и внешнего аудита ИБ. К этой группе документов относятся, например:

– реестры и описи;

– регистрационные журналы, в том числе журналы регистрации инцидентов;

– протоколы;

– листы ознакомления;

– обязательства;

– акты;

– договоры;

– отчеты.

Документы, содержащие свидетельства выполненной деятельности по обеспечению ИБ, могут быть представлены как в электронной форме, так и на бумажном носителе.

Должно обеспечиваться архивное хранение документов, содержащих свидетельства выполненной деятельности по обеспечению ИБ. Время хранения может определяться как требованиями законодательства РФ, так и требованиями ВНД.

9.10 Положения внутренних нормативных документов по обеспечению ИБ должны:

– носить не рекомендательный, а обязательный характер;

– быть выполнимыми и контролируемыми, не рекомендуется включать в состав этих документов положения, контроль реализации которых затруднен или невозможен;

– быть адекватными требованиям и условиям ведения деятельности (включая угрозы и риски ИБ), в том числе в условиях их изменчивости;

– не противоречить и не дублировать друг друга.

9.11 Менеджмент документов по обеспечению ИБ направлен на обеспечение разработки, учета, использования, хранения, проверки, обновления (поддержания актуального состояния) и изменения документов по обеспечению ИБ учреждения.

9.12 При осуществлении менеджмента документов по обеспечению ИБ необходимо:

– обеспечить адекватность документов перед их утверждением и изданием;

– периодически пересматривать и обновлять документы, а также утверждать их повторно;

– гарантировать возможность выявления изменений, вносимых в документы, и возможность определения текущего статуса документов;

– обеспечить уверенность в том, что требуемые документы доступны работникам учреждения, а его работники ознакомлены с требуемыми документами;

– обеспечить доступ к документам только тем работникам, которые имеют отношение к этим документам;

– обеспечить реализацию защиты документов от несанкционированного изменения;

– обеспечить уверенность в том, что документы удобочитаемы и идентифицируемы;

– предотвратить использование устаревших документов;

– использовать соответствующую маркировку для устаревших документов при их сохранении с какой-либо целью.

9.13 Менеджмент документов по обеспечению ИБ должен учитывать существующие требования законодательства РФ и ВНД учреждения.

10. Ответственность

10.1 Нарушение требований внутренних нормативных документов учреждения по обеспечению ИБ является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством РФ, ВНД учреждения, договорами, заключенными учреждением.

10.2 По степени опасности нарушения, связанные с несоблюдением требований ВНД по обеспечению информационной безопасности, делятся на две группы:

– нарушения, повлекшие за собой наступление нежелательных для учреждения последствий (утечку или уничтожение информации).

– нарушения, в результате которых созданы предпосылки, способные привести к нежелательным для учреждения последствиям (угроза уничтожения или утраты информации).

10.3 Лица, виновные в нарушениях требований ВНД в области ИБ, повлекших за собой нанесение ущерба учреждению, его клиентам и контрагентам несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

10.4 Степень ответственности за нарушение требований внутренних нормативных документов по обеспечению ИБ определяется, исходя из размера ущерба, причиненного учреждению.

10.5 Руководители подразделений учреждения несут персональную ответственность за:

– обеспечение ИБ в своем структурном подразделении;

– отражение в должностных обязанностях сотрудников требований обеспечения информационной безопасности на конкретном рабочем месте;

– доведение до сведения новых работников требований регламентирующих их деятельность по обеспечению ИБ при выполнении ими должностных обязанностей.

10.6 Работники учреждения обязаны выполнять требования ИБ и предписанные процедуры ИБ, в соответствии с их ролями в обеспечении ИБ. Каждый работник учреждения несет персональную ответственность за обеспечение информационной безопасности на своем рабочем месте.

11. Заключительные положения

11.1 Настоящая Политика вступает в силу с момента утверждения.

11.2 Настоящая Политика ИБ должна пересматриваться на этапе планирования СМИБ, а также в случаях изменения действующего законодательства РФ. Поводом для пересмотра Политики могут также являться результаты мониторинга и контроля состояния ИБ, анализа инцидентов ИБ, оценки (аудита) применяемых мер обеспечения ИБ или реализация угроз ИБ. В положениях политики ИБ должны быть учтены результаты оценки рисков ИБ.