ОПОИБ

4 курс, 9 группа, ММАД

1. Вариант

Крагель Алина

**Структура документов по безопасности информационных систем (Основные положения стандарта СТБ ISO/IEC 27002-2012). Документ "Безопасность при передаче информации и программного обеспечения. Безопасность других форм информационного обмена".**

Требования по обеспечению информационной безопасности при работе в автоматизированной системе должны быть отражены:

* во всех организационных документах организации, начиная с Устава, во всех положениях о структурных подразделениях организации
* в функциональных обязанностях всех сотрудников, участвующих в процессах автоматизированной обработки информации.

Задачи организации и функции по ОИБ ее подразделений и сотрудников в перечисленных выше документах должны формулироваться с учетом положений действующего законодательства по информатизации и защите информации, Указов Президента, Постановлений Правительства и других нормативных документов.

Конкретизация задач и функций структурных подразделений, а также детальная регламентация действий сотрудников организации, их ответственность и полномочия по вопросам ОИБ при эксплуатации АС должны осуществляться как путем дополнения существующих документов соответствующими пунктами, так и путем разработки и введения в действие дополнительных внутренних организационно-распорядительных документов по ОИБ.

Наиболее полную систему организационно-распорядительных документов по организации комплексной системы защиты информации можно создать в соответствии со стандартом СТБ ISO/IEC 27002-2012 «Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности», в котором определены Правила управления информационной безопасностью.

Стандарт СТБ ISO/IEC 27002-2012 устанавливает общие правила планирования, реализации, сопровождения и улучшения информационной безопасности в организации. Цели, оговоренные в стандарте, представляют собой общие руководящие принципы по регулярно принимаемым мерам менеджмента информационной безопасности. Цели и средства управления стандарта предназначены для реализации требований, выявленных оценкой рисков. Стандарт может служить в качестве практического руководства по разработке стандартов организаций по информационной безопасности и реализации эффективного менеджмента безопасностью, а также для обеспечения конфиденциальности при межорганизационном взаимодействии.

Документ "Безопасность при передаче информации и программного обеспечения. Безопасность других форм информационного обмена" предназначен для регламентации мер информационной безопасности при передаче информации. Вид документа – инструкция. Составляется подразделением безопасности и утверждается руководителем предприятия. Пересматривается и актуализируется по необходимости. Состав документа:

* Информирование персонала об угрозах информации при телефонных звонках:
* *близость посторонних людей при звонках по мобильным телефонам*
* *перехват звонков при физическом доступе к линии*
* *люди, находящиеся рядом с абонентом, принимающим звонок*
* Информирование персонала о недопустимости проведения конфиденциальных переговоров в общественных местах, открытых офисах или офисах с тонкими стенами
* Запрет на оставление конфиденциальных сообщений на автоответчиках
* Информирование персонала об угрозах информации при пользовании факсимильной связью:
* *неавторизованный доступ к месту получения сообщений*
* *запланированное или случайное программирование факса для посылки сообщений по определенным номерам*
* *посылка сообщений по неверным номерам*

**Организационное обеспечение информационной безопасности. Организационные и организационно-технические мероприятия: разовые, периодически проводимые и постоянно проводимые.**

Организационные (административные) меры регламентируют:

* процессы функционирования системы обработки данных,
* использование ее ресурсов, деятельность персонала, а также
* порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты являются той основой, которая объединяет различные меры защиты в единую систему.

Организационные и организационно-технические мероприятия включают:

* разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия;
* мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой АС или внешней среде (по необходимости);
* периодически проводимые (через определенное время) мероприятия;
* постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия.

Разовые мероприятия:

* мероприятия по созданию нормативно-методологической базы (разработка концепции и других руководящих документов) защиты АС;
* мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АС (исключение возможности тайного проникновения в помещения, исключение возможности установки прослушивающей аппаратуры и т.п.);
* мероприятия, осуществляемые при проектировании, разработке и вводе в эксплуатацию технических средств и программного обеспечения (проверка и сертификация используемых технических и программных средств, документирование и т.п.);
* проведение спецпроверок применяемых в АС средств ВТ и проведения мероприятий по защите информации от утечки по каналам побочных электромагнитных излучений и наводок;
* внесение необходимых изменений и дополнений во все организационно-распорядительные документы (положения о подразделениях, функциональные обязанности должностных лиц, технологические инструкции пользователей системы и т.п.) по вопросам обеспечения безопасности ресурсов АС и действиям в случае возникновения кризисных ситуаций;
* создание подразделения защиты информации (компьютерной безопасности) и назначение нештатных ответственных за ОИБ в подразделениях и на технологических участках, осуществляющих организацию и контроль за соблюдением всеми категориями должностных лиц требований по обеспечению безопасности программно-информационных ресурсов автоматизированной системы обработки информации, разработка и утверждение их функциональных обязанностей;
* мероприятия по разработке политики ИБ, определение порядка назначения, изменения, утверждения и предоставления конкретным категориям сотрудников (должностным лицам) необходимых полномочий по доступу к ресурсам системы;
* мероприятия по созданию системы защиты АС и необходимой инфраструктуры (организация учета, хранения, использования и уничтожения документов и носителей с закрытой информацией, оборудование служебных помещений сейфами (шкафами) для хранения реквизитов доступа, средствами уничтожения бумажных и магнитных носителей конфиденциальной информации и т.п.);
* мероприятия по разработке правил разграничения доступом к ресурсам системы (определение перечня задач, решаемых структурными подразделениями организации с использованием АС, а также используемых при их решении режимов обработки и доступа к данным;
* определение перечней файлов и баз данных, содержащих сведения, составляющие коммерческую и служебную тайну, а также требований к уровням их защищенности от НСД при передаче, хранении и обработке в АС;
* выявление наиболее вероятных угроз для данной АС, выявление уязвимых мест процессов обработки информации и каналов доступа к ней, оценка возможного ущерба, вызванного нарушением безопасности информации, разработку адекватных требований по основным направлениям защиты);
* организация охраны и надежного пропускного режима;
* определение порядка проектирования, разработки, отладки, модификации, приобретения, специсследования, приема в эксплуатацию, хранения и контроля целостности прогр. продуктов, а также порядок обновления версий используемых и установки новых сист. и прикл. программ на рабочих местах защищенной системы (кто обладает правом разрешения таких действий, кто осуществляет, кто контролирует и что при этом они должны делать),
* определение порядка учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные и т.п.;
* определение перечня необходимых регулярно проводимых превентивных мер и оперативных действий персонала по обеспечению непрерывной работы и восстановлению вычислительного процесса АС в критических ситуациях, возникающих как следствие НСД, сбоев и отказов СВТ, ошибок в программах и действиях персонала, стихийных бедствий.

Периодически проводимые мероприятия:

* распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);
* анализ системных журналов (журналов регистрации), принятие мер по обнаруженным нарушениям правил работы;
* пересмотр правил разграничения доступа пользователей к ресурсам АС организации;
* осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты и разработка необходимых мер по совершенствованию (пересмотру состава и построения) системы защиты.

Постоянно проводимые мероприятия:

* мероприятия по обеспечению) достаточного уровня физической защиты всех компонентов АС (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности СВТ, носителей информации и т.п.).
* мероприятия по непрерывной поддержке функционирования и управлению (администрированию) используемыми средствами защиты;
* организацию явного и скрытого контроля за работой пользователей и персонала системы;
* контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй, функционирования, обслуживания и ремонта АС;
* постоянно (силами службы безопасности) и периодически (с привлечением сторонних специалистов) осуществляемый анализ состояния и оценка эффективности мер и применяемых средств защиты.