|  |  |  |  |
| --- | --- | --- | --- |
|  | Ттермин (понятие) | Определение | ИСТОЧН ИК (ГОСТ, ОСТ, РД,  учебник, пособие,  статья,  др. источники) |
| п.п. |
|  |
|  |
|  | Защита информации | Деятельность по |  |
| 1 | предотвращению утечки защищаемой информации, несанкционированных и |  |
|  | непреднамеренных воздействий | [1] |
|  | на защищаемую информацию. |  |
|  | Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на: |  |
|  | 1)                 обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; |  |
|  | 2)                 соблюдение конфиденциальности информации ограниченного доступа; |  |
|  | 3)                 реализацию права на доступ к информации. |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  | [2] |
|  | Система защиты информации | Совокупность организационных мероприятий, технических, программных и |  |
| 2 | автоматизированной системы | программно-технических средств защиты информации и средств контроля эффективности защиты |  |
|  |  | информации. | [3] |
|  |  |  |  |
|  |  | Система защиты информации АС должна обеспечивать комплексное решение задач по защите информации от следующих угроз: |  |
|  |  |
| —                несанкционированный доступ (НСД) к информации АС; |  |
| —                утечка защищаемой информации по техническим каналам; |  |
| —                несанкционированные воздействия на информацию (на |  |
| носители информации); |  |
|  |  |
|  |  |
|  | [4] |
|  | Безопасность | Под информационной безопасностью РФ понимается состояние защищённости её национальных интересов и информационной сфере, определяющей совокупность интересов личности, общества и государства. В частности, среди основных задач, кои необходимо решить в области безопасности является обеспечение эффективного |  |
| 3 | компьютерной информации | функционирования электронного |  |
|  |  | бизнеса |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  | [5] |
|  |  | Практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от |  |
|  |  | формы, которую могут |  |
|  |  | принимать данные. | [6] |
|  |  |  |  |
|  | Метод защиты | На практике используют несколько групп методов защиты, в том числе: |  |
| 4 |  |  |
|  | препятствие на пути предполагаемого похитителя, которое создают физическими и программными средствами; |  |
|  | управление, или оказание воздействия на элементы защищаемой системы; |  |
|  | маскировка, или преобразование данных, обычно |  |
|  | – криптографическими способами; |  |
|  | регламентация, или разработка нормативно- правовых актов и набора мер, направленных на то, чтобы побудить пользователей, взаимодействующих с базами данных, к должному поведению; |  |
|  | принуждение, или создание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными; |  |
|  | побуждение, или создание условий, которые мотивируют |  |
|  | пользователей к должному |  |
|  | поведению. |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  | [7] |
|  |  |  |  |
|  |  | Методами и способами защиты информации от несанкционированного доступа являются: |  |
| - реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам; |  |
| - ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации; |  |
| - разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации; |  |
| - регистрация действий пользователей и обслуживающего персонала, контроль |  |
| несанкционированного доступа и действий пользователей, обслуживающего |  |
| персонала и посторонних лиц; |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | [8] |
|  |  |  |  |
|  | Механизм защиты | В NetWare реализованы три уровня защиты данных |  |
| 5 | Здесь под аутентификацией понимается: |  |
|  |  |  |
|  | -                     процесс подтверждения подлинности клиента при его подключении к сети, |  |
|  | -                     процесс установления подлинности пакетов, передаваемых между сервером и рабочей станцией. |  |
|  | Права по отношению к файлу (каталогу) определяют, какие операции пользователь может выполнить с файлом (каталогом). Администратор может для каждого клиента сети определить права по отношению |  |
|  | к любому сетевому файлу или |  |
|  | каталогу. |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  | [9] |
|  | Для защиты компьютерных систем от неправомерного вмешательства в процессы их функционирования и НСД к информации используются следующие основные методы зашиты: |  |
|  |  |
|  | -                     идентификация (именование и опознавание), аутентификация (подтверждение подлинности) пользователей системы; |
|  |  |
|  | -                     разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям; |
|  | -                     регистрация и |
|  |  |  |  |
|  |  | оперативное оповещение о событиях, происходящих в системе; (аудит) |  |
| [10] |
|  |  |  |  |
|  |  | -                     криптографическое закрытие хранимых и передаваемых по каналам связи данных; |  |
| -                     контроль целостности и аутентичности (подлинности и авторства) данных; |
| -                     выявление и нейтрализация действий компьютерных вирусов; |
| -                     затирание остаточной информации на носителях; |
| -                     выявление уязвимостей (слабых мест) системы; |
| -                     изоляция (защита периметра) компьютерных сетей (фильтрация трафика, скрытие внутренней структуры и адресации, противодействие атакам на внутренние ресурсы и т.д.); |
| -                     обнаружение атак и оперативное реагирование. |
| -                     Резервное копирование |
| -                     Маскировка. |
|  | Защита от | Это программные и/или аппаратные средства, позволяющие предотвратить попытки несанкционированного доступа, такие как неавторизованный физический доступ, доступ к файлам, хранящимся на компьютере, уничтожение конфиденциальных данных. |  |
| 6 | несанкционированного доступа |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  | [11] |
|  |  |  |  |
|  |  | Средства защиты от несанкционированного доступа (СЗИ от НСД) - программные, технические или программно- технические средства, предназначенные для предотвращения или существенного затруднения |  |
| несанкционированного доступа к |
| информации. |
|  |  |  |  |
|  |  | СЗИ от НСД может выполнять функции |  |
|  |  |
| -                     идентификация и аутентификация пользователей и устройств; | [12] |
| -                     регистрация запуска программ и процессов; |  |
| -                     реализация необходимых методов, типов и правил разграничения доступа; |  |
| -                     управление информационными потоками между устройствами; |  |
| -                     учет носителей информации и другие функции. |  |
|  | Фактор, воздействующий на защищаемую информацию | Явление, действие или процесс, результатом которых могут |  |
| 7 | быть утечка, искажение, уничтожение защищаемой |  |
|  | информации, блокирование | [13] |
|  | доступа к ней. |  |
|  |  |  |  |
|  |  | Под факторами, воздействующими на |  |
| защищаемую информацию, подразумевают явления, действия или процессы, результатом которых могут быть утечка, искажение, уничтожение защищаемой |
| информации или блокирование доступа к ней. |
|  |
| Различают объективные и субъективные факторы и в каждом классе выделяют |
| внешние и внутренние факторы. Подробный перечень факторов можно найти в ГОСТ Р 51275- 2006 (взамен ГОСТ Р 51275-99) , |
| который распространяется на требования по организации ЗИ при создании и эксплуатации объектов информатизации, используемых в |
| различных |
|  |  |  |  |
|  |  | областях деятельности (обороны, экономики, науки и других областях). | [14] |
|  |
| Значение некоторых используемых терминов: побочное электромагнитное излучение – излучение, возникающее при работе технических средств обработки информации; паразитное электромагнитное излучение – излучение, вызванное паразитной генерацией в электрических цепях технических средств обработки информации; «маскарад» – маскировка под зарегистрированного |
| пользователя. |
|  | Администратор защиты | Администратор безопасности является лицом, выполняющим функции по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники, в пределах своей зоны ответственности. |  |
| 8 | Изменение зоны |  |
|  | ответственности администратора безопасности производится приказом руководителя СИБ в случае изменения организационной структуры или по предложению СИБ. |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  | [15] |
|  |  |  |  |
|  | Способы управления безопасностью информационных технологий | Процесс управления безопасностью информационных технологий основывается на принципах, изложенных в ИСО/МЭК 13335- 1, и может быть реализован как в масштабе всей организации, так и в конкретной |  |
| 9 | ее части. На схеме |  |
|  | 1) приведены основные этапы этого процесса, а также показана обратная |  |
|  | связь между результатами процесса и его отдельными частями. Такая обратная связь должна устанавливается по мере необходимости как в пределах продолжительности одного из этапов, так и после завершения одного или нескольких этапов. |  |
|  | Данная схема демонстрирует основные направления, рассматриваемые в настоящем |  |
|  | стандарте. |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  | [16] |
|  | Цели и стратегия безопасности | В качестве первого шага в процессе управления безопасностью информационных технологий необходимо рассмотреть вопрос о том, какой общий уровень риска является приемлемым для данной организации. Правильно выбранный уровень приемлемого риска и, соответственно, допустимый уровень безопасности являются ключевыми моментами |  |
| 10 | информационных технологий | успешного управления |  |
|  |  | безопасностью. |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  | [17] |
|  |  |  |  |
|  | Политика безопасности | Политика безопасности информационных технологий должна вырабатываться на основе содержания |  |
| 11 | информационных технологий | стратегии и целей создания системы обеспечения безопасности. Важно сформировать политику безопасности и затем проводить ее в соответствии с направленностью деятельности организации, состоянием обеспечения безопасности, содержанием политики в области информационных технологий, а также с учетом положений законодательства и нормативных документов в области обеспечения |  |
|  |  | безопасности. |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  | [18] |
|  | Основные варианты стратегии анализа риска организации | Прежде чем приступить к любым действиям, связанным с анализом риска, организация должна иметь |  |
| 12 | стратегию проведения такого анализа, причем составные части этой стратегии (методы, способы и т.д.) |  |
|  | должны быть отражены в содержании политики обеспечения безопасности информационных технологий. Эти методы и критерии выбора вариантов стратегии анализа риска должны отвечать потребностям организации. |  |
|  | Стратегия анализа риска должна обеспечивать соответствие |  |
|  | выбранного варианта стратегии условиям осуществления деловых операций и приложения усилий по обеспечению безопасности в тех |  |
|  | областях, где это действительно |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  | [19] |
|  |  |  |  |
|  |  | необходимо. |  |