

Решения "Кода Безопасности" для защиты персональных данных

При проектировании безопасности персональных данных требуется рассматривать угрозу загрузки с внешних носителей в процессе загрузки операционной системы. В системах К1 все оцениваемые угрозы являются актуальными по причине высокого уровня показателя опасности угрозы в силу определения самого класса системы персональных данных, как класса К1. Это делает показатель возможности реализации угрозы в К1 нерелевантным при определении актуальности угрозы. Все угрозы системы К1 всегда будут актуальными вне зависимости от возможности их реализации.

Актуальность угрозы загрузки с внешних носителей для информационных систем класса К2 будет определяться в процессе проектирования системы безопасности с учетом среднего уровня показателя опасности угрозы. Фактически угроза может быть признана неактуальной только в системах с высокой степенью исходной защищенности и в некоторых системах со средней степенью исходной защищенности, где реализация угрозы будет признана маловероятной, таким образом, есть основания полагать, в большинстве систем К2 угроза будет признана актуальной.

В настоящий момент компания "Код Безопасности" представляет набор аппаратных средств защиты, нейтрализующих угрозу загрузки с внешних носителей информации

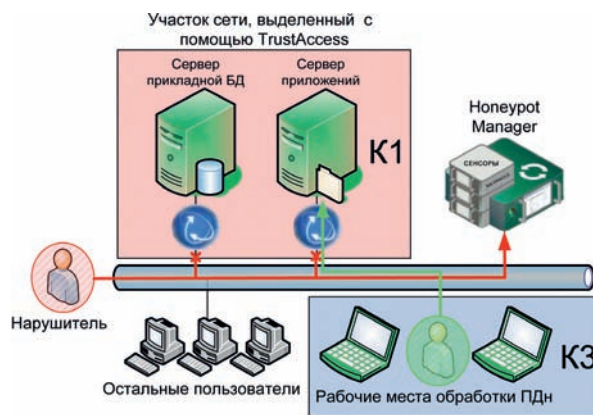
Электронный замок "Соболь" – это аппаратно-программное средство защиты компьютера от несанкционированного доступа (модуль доверенной загрузки). "Соболь" может применяться как устройство, обеспечивающее защиту автономного компьютера, а также рабочей станции или сервера в составе локальной вычислительной сети.

Secret Net Touch Memory Card представляет собой плату PCI/PCI Express

и позволяет осуществлять аппаратную поддержку процедуры идентификации и аутентификации пользователей с помощью электронных идентификаторов iButton и запрет несанкционированной загрузки операционной системы с внешних съемных носителей.

Защита от программно-математических воздействий

Программно-математическое воздействие (ПМВ) – это несанкционированное воздействие нарушителя на ресурсы информационных систем персональных данных, осуществляемое с помощью специальных вредоносных программ, и ставящее целью получение несанкционированного доступа к инфор-



мации. Обычно такие вредоносные программы эксплуатируют известные нарушителю уязвимости ПО, используемого в информационной системе.

Согласно требованиям документов ФСТЭК для защиты ИСПДн К1 и К2 должны применяться комбинированные методы обнаружения атак на базе имитаторов персональных данных на основе специальных модулей-ловушек.

"Код Безопасности" представляет следующие средства данного класса:

1) **СЗИ от ПМВ Honeypot Manager** – первая система имитации персональных данных на базе специальных ловушек, специально созданная в соответствии с требованиями документов ФСТЭК;

2) продукт **Security Studio Suite** – комплексная защита персональных данных на рабочих местах, включающая в себя следующие компоненты:

- безопасный доступ в сеть – межсетевой экран с контролем трафика пресекает попытки несанкционированного доступа к защищаемой информации из локальной сети или Интернета;
- антивирусная защита – быстрый и эффективный сканер, сочетающий в себе антивирус и антишпион, автоматически обнаруживает и обезвреживает или удаляет вредоносное ПО;
- защита от ПМВ – модуль "локальная безопасность" – контролирует взаимодействие программ, предотвращая неизвестные или подозрительные операции, позволяя защитить систему от нераспознаваемых угроз;
- защита от отключения системы безопасности – вирусы и хакеры не смогут отключить работу системы защиты, благодаря чему она всегда будет оставаться на страже безопасности;
- дополнительные модули "Веб-контроль" и "Антиспам" оградят от угроз Интернета, включая риски обращения к вредоносному контенту веб-серверов и кражи личных данных.

Можно приобрести отдельные компоненты системы для закрытия определенных требований по защите персональных данных. **Security Studio Suite** обеспечивает защиту ИСПДн до класса К1.

Защита сетевых приложений и сервисов, обрабатывающих информацию ограниченного доступа

Персональные данные часто обрабатываются не на локальных компьютерах, а на серверах баз данных, в клиентских приложениях, использующих сетевые сервисы (такие как внутрикорпоративные веб-сервисы или серверы приложений), в веб-приложениях и т.п. Традиционные СЗИ от НСД, созданные на базе требований к автоматизированным системам, сконцентрированы на защите локальных конфиденциальных файловых ресурсов. Используя традиционное СЗИ от НСД, пользователь аутентифицируется на локальном АРМ, и эта аутентичность достоверна только на данном рабочем месте. Требуется использование механизма доверенной сетевой аутентификации и авторизации пользователя, вошедшего в систему на одном компьютере сети, к сетевому сервису на другом компьютере сети. В компании "Код Безопасности" разработан продукт **TrustAccess** для сетевого разграничения доступа, созданного для реализации требований ФСТЭК. Представляет собой систему распределенных межсетевых экранов 2-го класса защиты с централизованным управлением и предназначен для защиты сетевых ресурсов информационной системы от НСД.