УДК 004.056.53

Список сокращений.

АРМ - автоматизированной рабочее место;

АС - автоматизированная система;

ЗИ от НСД - защита информации от несанкционированного доступа;

ЛВС - локально вычислительная сеть;

МЭ - межсетевой экран;

ОИ - объект информатизации;

ПЭВМ - персональная электронно вычислительная машина;

СЗИ от НСД - средство защиты информации от несанкционированного доступа.

Герасимов А.А. Email: ger-anton@mail.ru

Кузнецов В.А. Email: viktor__kuznetsov@mail.ru

Мозговой А.В. Email: runc.nsd@gmail.com

Пугачев К.А. Email: pugachev_ka13@mail.ru

Основные подсистемы СЗИ от НСД и особенности их настройки на АС.

Аннотация.

В данной статье представлен обзор существующих типов обеспечения ЗИ от НСД на ОИ. Рассматриваются основные требования предъявляемые к СЗИ от НСД. Описываются основные подсистемы работы СЗИ от НСД, а также рекомендации по настройке этих подсистем. Сделан вывод о корректности и адекватности применения правильно настроенного комплекса СЗИ от НСД.

Ключевые слова: защита информации, несанкционированный доступ, объект информатизации, автоматизированная система, средство защиты информации.

List of reductions.

AW - automated workplace;

AS - the automated system;

IS from UA - information security from unauthorized access;

LAN - locally computer network;

ME - the firewall;

OI - object of informatization;

PC - personal computer;

ISM from UA - information security measure from unauthorized access.

Gerasimov A.A. Email: ger-anton@mail.ru

Kuznetsov V.A. Email: viktor__kuznetsov@mail.ru

Brain A.V. Email: runc.nsd@gmail.com

Pugachev K.A. Email: pugachev_ka13@mail.ru

The main subsystems of ISM from UA and feature of their control on the AS.

Summary.

The review of existing types of providing IS is presented in this article from US on OI. The main demands made to ISM from UA are considered. Subsystems of work of ISM from UA, and also recommendations about control of these subsystems are described by the main. The conclusion is drawn on a correctness and adequacy of application of correctly adjusted ISM complex from UA.

Keywords: information security, unauthorized access, object of the informatization, the automated system, information security measure.

ЗИ от НСД на ОИ представляет собой важную составляющую обеспечения безопасности информации на ОИ. В отличие от других факторов обеспечения безопасности информации, таких как защита информации от

утечки по техническим каналам, несмотря на также законодательно фиксированные требования к ЗИ от НСД информации определенного уровня конфиденциальности, при ЗИ от НСД применяется более творческий подход к построению системы защиты.

В настоящее время в зависимости от типа ОИ и его структуры для обеспечения ЗИ от НСД могут применяться следующие классы средств защиты:

1. Средства аппаратной идентификации;
2. Средства антивирусной защиты;
3. Средства обнаружения вторжений;
4. Межсетевые экраны;
5. Программные и программно-аппаратные СЗИ от НСД;
6. Средства шифрованы.

Построение комплекса по ЗИ от НСД на каждом конкретном ОИ начинается с построения модели информационного документооборота ОИ. Проводиться изучение информационных потоков на ОИ, определяются риски и основные угрозы информации на всех этапах ее хранения, обработки и передаче на ОИ. На основании полученной информации строится матрица доступа к информации обрабатываемой в ОИ, а также схема информационных потоков. На основании собранных об ОИ сведений строится модель комплекса СЗИ от НСД для исследуемого ОИ.

Чаще всего АРМ в составе ОИ применяются программные или программно-аппаратные СЗИ от НСД. В зависимости от того имеются ли у

АРМ в составе ОИ сетевые подключения принимается решении о применении средств межсетевого экранирования, а также средств обнаружения вторжений.

Основную же роль в обеспечении безопасности на ОИ играет СЗИ от НСД. В данный момент на рынке средств защиты предлагается обширный выбор СЗИ от НСД, основными из которых являются:

1. Аккорд;
2. Страж;
3. Secret net;
4. Dallas lock.

Каждое из приведенных выше средств отличается своими особенностями в работе. В связи с тем, что все эти средства имеют действующие сертификаты соответствия ФСТЭК России по защите информации на АС ОИ до класса 1Б включительно, положительно или отрицательно оценивать средства можно по двум критериям: удобство в работе для пользователя, удобство и прозрачность настройки.

Согласно Руководящему документу "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" СЗИ от НСД должно обеспечивать безопасность информации следующими четырьмя основными подсистемами:

1. Подсистема идентификации и аутентификации;
2. Подсистема регистрации и учета;
3. Подсистема криптографической защиты;

4. Подсистемами обеспечения целостности.

Подсистема идентификации и аутентификации предоставляет и контролирует доступ к работе на АРМ ОИ пользователей. В зависимости от уровня конфиденциальности информации и от класса АС, на которой эта информация обрабатывается, могут применяться разные методы идентификации и аутентификации. Однако, стоит отметить, что одним из самых надежных методов является аппаратная идентификация с последующей аутентификацией по паролю определенной длины и сложности в зависимости от класса АС.

Основными задачами подсистемы регистрации и учета является ведение журнала всех действий пользователя на АРМ АС, фиксация в журнал попыток НСД пользователя к ресурсам, доступ к которым ему запрещен, учет всех носителей информации и гарантированное уничтожение затираемой информации. Основным уязвимым местом работы АС являются съемные носители. Связано это в первую очередь с тем, что для удобной работы пользователи часто пренебрегают некоторыми принципами защиты информации и начинают применять в своей работе съемные носители разного рода и происхождения. Естественно, что при этом возникает риск заражения АРМ АС компьютерными вирусами, а также утечки информации с использованием незарегистрированных носителей. На упразднение данной угрозы и направлена работа подсистемы регистрации учета СЗИ от НСД. Чаще всего в СЗИ жестко фиксируется набор носителей по их заводскими номерам, определяемым при подключении к АРМ, и список атрибутов по доступу к ним.

Это позволяет избежать несанкционированного копирования информации и как результат утечки ее с использованием сторонних носителей, а также избежать заражения АРМ АС компьютерными вирусами. Однако, при настройке данной подсистемы, необходимо тщательно изучить процесс работы пользователей АС, так как жесткая настройка без учета тонкостей циркуляции информации может привести к значительному снижению удобства применения СЗИ от НСД конечными пользователями, а как результат, новых попыток НСД ими.

Подсистема криптографической защиты преобразовывает информацию обрабатываемую в АС с использованием известных надежных криптографических алгоритмов. Применение данной подсистемы определяется классом АС, а также тем, как циркулирует информация на АС. Чаще всего информация зашифровывается при передаче по сети и реже при ее сохранении на съемные носители.

Основной задачей подсистемы контроля целостности является сохранение работоспособности как программной, так и аппаратной части АС. Причем согласно Руководящему документу "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" все требования предъявляемые здесь к АС СЗИ от НСД не в состоянии реализовать. Такими являются требование физической охраны средств АС и наличие администратора безопасности. Что же касается СЗИ от НСД, то в ее обязанности входит подсчет контрольных сумм программного обеспечения АС и контроль аппаратной конфигурации АС. В случае несовпадения контрольных

сумм и/или изменения аппаратной конфигурации компьютера работа текущего пользователя блокируется. Контроль производится в два этапа: по завершении работы пользователя СЗИ от НСД вычисляет контрольные суммы программ и сохраняет аппаратную конфигурацию АС, при включении АРМ АС в следующий раз на этапе загрузка Операционной системы и СЗИ от НСД происходит сравнение контрольных сумм и аппаратной конфигурации с эталонными значениями. По результатам сравнения принимается решение о возможности дальнейшей работы пользователя на АС.

Как видно из вышесказанного, настройка СЗИ от НСД зависит от многих факторов. И именно грамотный учет всех тонкостей работы с информацией на АС, а также анализ угроз безопасности информации и соблюдение требований руководящих документов обеспечивает ЗИ от НСД в АС и, что немаловажно, обеспечивает удобную, комфортную работу пользователей.