**Дьячков Виктор Васильевич,**
генеральный директор компании «ICL — КПО ВС»

# Комплексная интеграция средств защиты информации с целью повышения эффективности работы сотрудников МВД России

Компания «АйСиЭл — КПО ВС» уже более 20 лет является надежным поставщиком программных и технических решений для нужд правоохранительных органов и является признанным интегратором в области создания сложных крупных защищенных автоматизированных систем государственного назначения.

Накопленный за это время опыт внедрения и интеграции разнородных средств защиты информации позволяет сделать вывод о наличии ряда проблемных вопросов, препятствующих эффективному использованию средств защиты информации сотрудниками информационных центров МВД России.

В данной статье рассматриваются типовые проблемы и вопросы использования средств защиты информации применительно к существующим в МВД России автоматизированным системам, а также предлагаются возможные пути решения и перспективы их развития.

В качестве объекта автоматизации будем рассматривать только автоматизированные системы, обрабатывающие персональные данные. Защита информации, составляющей государственную тайну, имеет свою специфику и должна являться темой отдельной статьи.

Рассмотрим типовую комплексную автоматизированную систему, использующуюся в МВД России.

**Данная автоматизированная система, как правило, содержит в своем составе следующие типовые элементы:**

- сервера СУБД;
- сервера приложений;
- инфраструктурные сервера;
- сетеобразующее оборудование;
- разнородные и несвязанные средства защиты информации, без объединения в комплексную систему;
- клиентские автоматизированные рабочие места.

В большинстве случаев сервера СУБД обрабатывают персональные данные высшей и 1 категории, а с использованием дополнительных средств защиты информации клиентские автоматизированные места обрабатывают персональные данные 2 или 3 категории.

Поскольку уровень защищенности объекта защиты равен уровню защищенности самого слабого компонента средств защиты, то для надежной защиты потребуется комплексная система защиты информации.

**Для рассмотренного объекта защиты могут быть выделены следующие подсистемы:**

- идентификации и аутентификации;
- управления доступом;
- контроля целостности;
- резервного копирования;
- мониторинга и реагирования;
- криптографическая подсистема;
- антивирусная подсистема.

**Данная комплексная система, в общем случае, будет включать в свой состав следующие средства защиты информации:**

1. защищенные операционные системы;
2. средства защиты информации служб каталогов;
3. программные средства защиты информации от несанкционированного доступа для серверов;
4. антивирусные средства;
5. средства доверенной загрузки, аппаратно-программные модули доверенной загрузки (АПМДЗ);
6. средства обнаружения вторжений;
7. программно-аппаратные устройства усиленной аутентификации;
8. средства мониторинга и анализа защищенности;
9. средства криптографической защиты каналов связи;
10. средства VPN-туннелирования;
11. средства межсетевого экранирования.

Также возможно использование дополнительных средств резервного копирования, средств контроля целостности, средств-ловушек злоумышленников (honeypot) и иных средств защиты информации.

Таким образом, количество разнородных средств защиты информации может достигать 14 и более, и при этом в большинстве случаев у каждого применяемого средства защиты информации свой отдельный производитель.

Соответственно возникает проблема обучения сотрудников МВД России, ответственных за функционирование объекта защиты. Минимально необходимый объем знаний, требуемый даже для базового администрирования объекта защиты информации, является колоссальным, не говоря уже о выполнении сложных задач по восстановлению информации в случае возникновения каких-либо инцидентов защиты информации. В дополнение необходимо отметить, что на текущий момент наблюдается нехватка личного состава и зачастую количество выполняемых сотрудниками ИЦ МВД России функций превышает разумные пределы.

Вышеперечисленные проблемы могут быть решены за счет покупки у производителей средств защиты или компаний-интеграторов технической поддержки, данные фирмы имеют все необходимые лицензии на выполнение работ и обладают штатом высококвалифицированных специалистов. **Однако, наряду с очевидными плюсами, данное решение имеет как минимум два недостатка:**

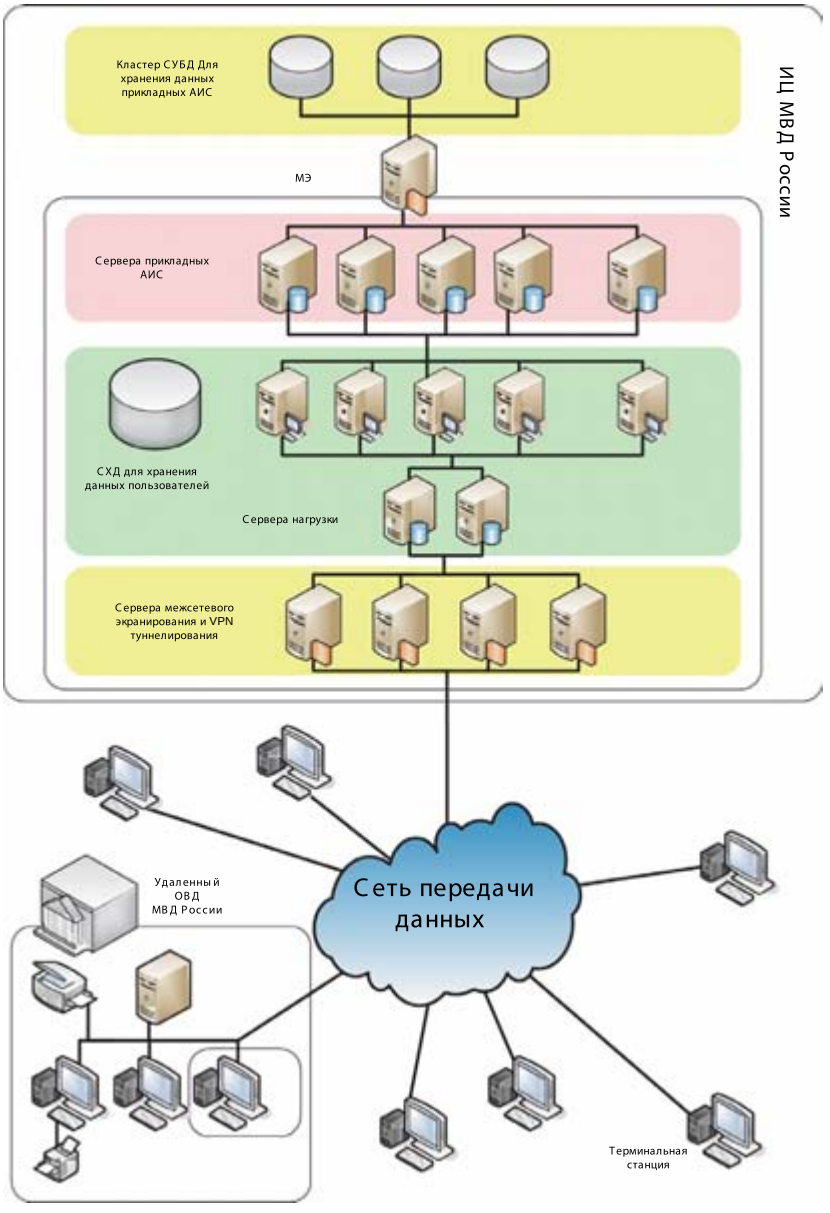
- относительно высокая стоимость технического обслуживания;
- необходимость предоставления доступа к оборудованию (и потенциально, к информационным ресурсам) лицам, не являющимся сотрудниками МВД России, что влечет за собой риск утечки и компрометации защищаемой информации.

Наиболее эффективным решением является обучение сотрудников ИЦ МВД России навыкам и знаниям, необходимыми для администрирования средств защиты.

Но каким образом можно качественно обучить ответственного за администрирование объекта защиты информации сотрудника работе с различными и разнородными средствами защиты информации?

В качестве ответа на данный вопрос предлагается решение по созданию комплексной системы управления средствами защиты информации, обеспечивающей унифицированных подход к администрированию разнородных средств защиты информации.

Необходимо отметить, что такой унифицированный подход может быть разработан, т.к. для возможности использования средств защиты информации на объекте автоматизации в первую очередь необходимо наличие сертификата на указанное средство защиты информации. А поскольку сертификация проводится в большинстве случаев на соответствие требованиям нормативных документов Гостехкомиссии (ФСТЭК) Рос-




сии (руководящие документы для средств вычислительной техники, автоматизированных систем, межсетевых экранов), то имеется возможность выделения общих принципов администрирования средств защиты информации.

**Комплексная система администрирования средствами защиты информации (КСАСЗИ) обеспечит следующие дополнительные преимущества:**

1. наличие единого унифицированного графического интерфейса, что позволит значительно упростить процесс мониторинга и управления объектом защиты информации;
2. возможность лучшего контроля объекта защиты за счет объединения информации, поступающей от различных средств защиты информации;
3. снижение затрат на обучение и администрирование;
4. упрощение и качественное выполнение регламентных задач;
5. снижение затрат на модернизацию системы защиты информации;
6. ускорение времени реакции на возникающие инциденты защиты информации;
7. возможность создания отчетов и анализа информации от разнородных средств защиты информации.

В конечном счете применение КСАСЗИ повысит уровень защищенности систем, т.к. администраторы безопасности будут лучше понимать и видеть «целиком» весь объект защиты информации.

Очевидно, что большинство производителей средств защиты информации негативно воспримут идею создания комплексной системы администрирования, т.к. данное решение потенциально влечет частичный отказ от платной технической поддержки производителя.

**Поэтому решение данного вопроса должно исходить от заказывающего департамента МВД России. Предположительный порядок работ должен быть следующий:**

- Проведение НИР на выполнение работ по созданию КСАСЗИ, результатом которого формируется отчет о НИР, в котором должен содержаться анализ существующих средств защиты информации, должны быть выделены унифицированные подсистемы, а также разработана архитектура КСАСЗИ. Должны быть разработаны протоколы взаимодействия средств защиты с КСАСЗИ.
- Передача протоколов взаимодействия всем крупнейшим разработчикам средств защиты информации с целью использования в своих последующих разработках.
- Проведение работ по созданию и внедрению КСАСЗИ.
- Требование использования протоколов взаимодействия для всех последующих конкурсов по созданию крупных защищенных автоматизированных систем.

Необходимо отметить, что отчасти похожие системы унифицированного администрирования существуют у крупнейших зарубежных компаний (IBM Tivoli, CA Unicenter Network and Systems Management, HP OpenView, Microsoft System Center и т.д.). Однако указанные системы ориентированы в первую очередь на администрирование сетей крупных предприятий, не учитывают специфику отечественных средств защиты и не обладают сертификатами защиты информации. Поэтому необходимо говорить именно о создании нового средства, направленного на решение конкретных задач сотрудников МВД России.

С точки зрения сроков, указанное решение может быть разработано в течение одного с половиной года (с учетом проведения НИР и разработки самой системы).