



Код безопасности  
ГК «Информзащита»

## Снижение класса ИСПДн и уровня АС через сегментирование сети

Статья содержит описание принципов работы и преимуществ Honeypot-систем, их места в общей системе безопасности, а также описывает новый продукт компании – Security Studio Honeypot Manager.

## Выделение сервера в отдельный сегмент сети

Согласно [4]: «Выбор и реализация методов и способов защиты информации в информационной системе осуществляются на основе определяемых оператором (уполномоченным лицом) угроз безопасности персональных данных (модели угроз) и в зависимости от класса информационной системы, определенного в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. N 55/86/20.»

Классификация ИСПДн проводится на этапе их создания или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и средств защиты информации, необходимых для обеспечения безопасности персональных данных.

**В случае выделения в составе информационной системы подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.**

Результаты классификации информационных систем оформляются соответствующим актом оператора».

Таким образом, именно оператор выполняет классификацию своей ИСПДн, определяет ее состав, конфигурацию и меры по защите. Следовательно, оператор вправе выполнить сегментирование большой ИСПДн высокого класса на отдельные взаимодействующие ИСПДн разных классов.

Согласно [5]: 5.1.7. «Если объединяются АС различных классов защищенности, то интегрированная АС должна классифицироваться по высшему классу защищенности входящих в нее АС, за исключением случаев их объединения посредством межсетевых экранов, когда каждая из объединяющихся АС может сохранять свой класс защищенности». 5.8.4. «Подключение ЛВС к другой автоматизированной системе (локальной или

**неоднородной вычислительной сети) иного класса защищенности должно осуществляться с использованием МЭ, требования к которому определяются РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».**

Согласно [4, раздел II, пункт 2.4] «При взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с методами и способами, указанными в пункте 2.1 настоящего Положения, основными методами и способами защиты информации от несанкционированного доступа являются:

межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы...».

Согласно [4, раздел III, пункты 2.4, 3.3, 4.4] «Безопасное межсетевое взаимодействие для ИСПДн при их подключении к сетям международного информационного обмена, а также для распределенных ИСПДн при их разделении на подсистемы достигается путем применения средств межсетевого экранирования (межсетевых экранов), который реализуется программными и программно-аппаратными межсетевыми экранами (МЭ). Межсетевой экран устанавливается между защищаемой сетью, называемой внутренней, и внешней сетью. Межсетевой экран входит в состав защищаемой сети. Для него путем настроек отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот. Для обеспечения безопасного межсетевого взаимодействия в ИСПДн 3 и 4 классов рекомендуется использовать МЭ не ниже пятого уровня защищенности. Для обеспечения безопасного межсетевого взаимодействия в ИСПДн 2 класса рекомендуется использовать МЭ не ниже четвертого уровня защищенности. Для обеспечения безопасного межсетевого взаимодействия в ИСПДн 1 класса рекомендуется использовать МЭ не ниже третьего уровня защищенности».<sup>1</sup>

<sup>1</sup> Исходя из сравнения требований к МЭ в документе [7].

## Цитата из Приложения 1 к Письму Рособразования от 22.10.2009 N 17-187 «Об обеспечении защиты персональных данных» [6]:

**«5. Понижение требований по защите персональных данных путем сегментирования ИСПДн.**

**Сегментирование** заключается в разделении сетевой ИСПДн на несколько сегментов для уменьшения требований и упрощения защиты персональных данных. Оно позволяет:

– децентрализовать обработку персональных данных 2-й категории и понизить класс сегментов ИСПДн до К3, если количество субъектов персональных данных превышает 1000 человек, или если они не принадлежат организации-оператору.

– уменьшить количество защищаемых АРМ в распределенных ИСПДн.

**Данный способ на практике является одним из основных.**

При сегментировании ИСПДн на взаимодействующие по сети подсистемы следует иметь в виду, что класс системы в целом равен наиболее высокому классу ее подсистем (сегментов). Поэтому **простое разделение на ИСПДн подсистемы без ограничения их взаимодействия не снижает требования по защите персональных данных.**

Простейшим способом ограничения взаимодействия сегментов является их физическое (гальваническое) изолирование друг от друга. Альтернативным способом сегментирования является использование сертифицированных ФСТЭК России межсетевых экранов».

Следовательно, при сегментировании ИСПДн, в результате которого появляются составные взаимодействующие ИСПДн разных классов (согласно процедуре классификации ИСПДн), эти составные ИСПДн сохраняют свой индивидуальный класс (уровень защищенности), если будут разделены межсетевыми экранами соответствующих классов.

## Сегментирование до уровня отдельных АРМ

Выделять отдельное АРМ, не являющееся сервером, в отдельную ИСПДн имеет смысл, когда:

1. Необходимо понизить класс системы на конкретном АРМ.
2. АРМ, исходя из количественного критерия, содержит данные К3 или К2, но из-за того, что количество таких АРМ в одном сегменте сети велико, система в целом достигает более высокого уровня – К2 или К1.

Для решения этой проблемы можно применять сегментирование до уровня отдельного АРМ с помощью персонального межсетевого экрана (ПМЭ) соответствующего уровня. Важным условием является следующий момент.

Установка ПМЭ на АРМ, не являющимся сервером, приводит к появлению отдельного сегмента сети, состоящего из одного АРМ. При установке на это АРМ сертифицированного СЗИ от НСД Secret Net можно гарантировать, что на этом АРМ может работать только один пользователь одновременно. С помощью сертифицированного СЗИ от НСД можно также гарантировать, что пользователи, работающие на этом АРМ в разное время, не смогут получить доступ к данным друг друга. Обычно для офисных сетей характерна ситуация, когда работа более чем одного пользователя на некотором АРМ не предусмотрена. В дальнейшем будем рассматривать именно этот сценарий.

В этом случае отдельное АРМ, выделенное в отдельный сегмент, следует рассматривать как отдельную однопользовательскую ИСПДн с данными, расположенными локально на этом АРМ (временные файлы клиента базы данных, экспортированные выписки после получения отчетов и т.д.).

**Здесь важно гарантировать, что ИСПДн действительно является однопользовательской, т. е. другие пользователи сети не могут обратиться к персональным данным на АРМ ни локально, ни удаленно через сеть. Локальный доступ ограничивается сертифицированным СЗИ от НСД. Сетевой доступ можно заблокировать через блокировку всех (исключая служебный трафик) входящих соединений на ПМЭ. Поскольку АРМ не**

**является сервером, это не должно представлять проблему с точки зрения бизнес-процессов.**

Далее есть два принципиально различающихся варианта:

- **2.1 АРМ НЕ подключено к сетям общего доступа (Интернет):**

В этом случае согласно [4] какие-либо специальные требования на межсетевое экранирование ИСПДн отсутствуют и при выборе уровня ПМЭ, обеспечивающего сегментирование, следует руководствоваться документом [4].

«Для обеспечения безопасного межсетевого взаимодействия в ИСПДн 3 и 4 классов рекомендуется использовать МЭ *не ниже пятого уровня защищенности*. Для обеспечения безопасного межсетевого взаимодействия в ИСПДн 2 класса рекомендуется использовать МЭ *не ниже четвертого уровня защищенности*. Для обеспечения безопасного межсетевого взаимодействия в ИСПДн 1 класса рекомендуется использовать МЭ *не ниже третьего уровня защищенности*».<sup>2</sup>

Таким образом:

Для выделения отдельного АРМ, не являющегося сервером, в отдельную ИСПДн, при отсутствии подключения к сетям общего доступа, необходимо в части разграничения доступа:

1. Установить сертифицированное СЗИ от НСД
2. Установить сертифицированный ПМЭ и заблокировать на нем все входящие соединения, исключая служебный трафик. ПМЭ должен иметь сертификат на МЭ не ниже:
  - a. 5 класса – для К3
  - b. 4 класса – для К2
  - c. 3 класса – для К1

- **2.2 АРМ подключено к сетям общего доступа (Интернет)**

В этом случае, согласно [4] предусмотрены специальные требования к межсетевому экранированию даже однопользовательской системы, которые сводятся к требованию сертифицированного МЭ не ниже 4 класса – для ИСПДн класса К3 и МЭ не ниже 4 и 3 класса – для ИСПДн класса К2 или К1 соответственно.

В данном случае также имеет смысл гарантировать однопользовательский режим за счет блокирования всех входящих соединений, исключая служебный трафик.

<sup>2</sup> Исходя из сравнения требований к МЭ в документе [7].

Таким образом, для выделения отдельного АРМ, не являющегося сервером, в отдельную ИСПДн, при наличии подключения к сетям общего доступа, необходимо в части разграничения доступа:

1. Установить сертифицированное СЗИ от НСД
2. Установить сертифицированный ПМЭ и заблокировать на нем все входящие соединения, исключая служебный трафик. ПМЭ должен иметь сертификат на МЭ не ниже:
  - а. 4 класса – для К3
  - б. 4 класса – для К2
  - в. 3 класса – для К1

Таблица 1. Сводная таблица требований к уровню защищенности ПМЭ, для выделения отдельного АРМ в отдельный сегмент ИСПДн самостоятельного класса.

Класс ИСПДн на АРМ	Подключение АРМ к сетям общего доступа (Интернет)	
	Нет	Есть
К3	МЭ 5	МЭ 4
К2	МЭ 5	МЭ 4
К1	МЭ 4	МЭ 3

## Шифрование сетевого трафика между сегментами сети

Дополнительно следует рассмотреть вопрос о необходимости применения криптографических средств между взаимодействующими ИСПДн (сегментами одной сети).

При защите персональных данных по линии ФСТЭК необходимо иметь в виду, что криптографическая защита информации в общем случае не регламентируется ФСТЭК. Например, согласно п. 1.27 документа [5]: «Техническая защита конфиденциальной информации – защита информации некриптографическими методами, направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и от специальных воздействий на информацию в целях ее уничтожения, искажения или блокирования». То же самое есть и в документе [4]: «Обеспечение безопасности ПДн с использованием криптографических методов в настоящем документе не рассматривается. Порядок организации и обеспечения указанных работ определяется в соответствии с нормативными документами Федераль-

ной службы безопасности Российской Федерации».

Вместе с тем согласно п. 5.2.5 документа [5]: «Для передачи информации по каналам связи, выходящим за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи, а при использовании открытых каналов связи, применять криптографические средства защиты информации. Применяемые средства защиты информации должны быть сертифицированы».

Согласно терминам документов ФСТЭК: «Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств».

Таким образом, если образовавшиеся в результате сегментирования сегменты сети находятся в пределах контролируемой зоны, криптографическая защита каналов связи между ними согласно требованиям ФСТЭК НЕ требуется.



## Код безопасности

ГК «Информзащита»

Почтовый адрес: 127018, Россия, Москва, а/я 55.

Адрес офиса в Москве: ул. Образцова, д. 38.

Адрес офиса в Санкт-Петербурге: Свердловская наб., д. 44.

Тел.: +7 (495) 980-2345 (многоканальный).

Факс: +7 (495) 980-2345.

E-mail: [info@securitycode.ru](mailto:info@securitycode.ru)

Запрос дополнительной информации о продуктах: [info@securitycode.ru](mailto:info@securitycode.ru)

По вопросам стоимости и покупки продуктов [sales@securitycode.ru](mailto:sales@securitycode.ru)

По вопросам партнерства и сотрудничества [info@securitycode.ru](mailto:info@securitycode.ru)

Вы можете узнать подробную информацию о продуктах на сайте

[www.securitycode.ru](http://www.securitycode.ru)

### **О компании «Код Безопасности»**

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, коммерческой и государственной тайны, а также среды виртуализации. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

«Код Безопасности» входит в группу компаний «Информзащита», которая уже около 15 лет является лидером российского рынка информационной безопасности.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.