Об утверждении Профилей защиты и Методики разработки профилей защиты

Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 27 июня 2018 года № 105/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 30 июля 2018 года № 17247

В соответствии с подпунктом 18) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" ПРИКАЗЫВАЮ:

1. Утвердить:

1) Профили защиты средств антивирусной защиты для рабочих станций и серверов, а также систем обнаружения вторжений уровня сети, согласно приложению 1 к настоящему приказу;

2) Методики разработки профилей защиты согласно приложению 2 к настоящему приказу.

2. Комитету по информационной безопасности Министерства оборонной и аэрокосмической промышленности Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

1) государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан;

2) в течение десяти календарных дней со дня государственной регистрации настоящего приказа направление его копии в бумажном и электронном виде на казахском и русском языках в Республиканское государственное предприятие на праве хозяйственного ведения "Республиканский центр правовой информации" для официального опубликования и включения в Эталонный контрольный банк нормативных правовых актов Республики Казахстан;

3) в течение десяти календарных дней после государственной регистрации настоящего приказа направление его копии на официальное опубликование в периодические печатные издания;

4) размещение настоящего приказа на официальном интернет-ресурсе Министерства оборонной и аэрокосмической промышленности Республики Казахстан после его официального опубликования;

5) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства оборонной и аэрокосмической промышленности Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1), 2), 3) и 4) настоящего пункта.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра оборонной и аэрокосмической промышленности Республики Казахстан.

4. Настоящий приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Министр оборонной и аэрокосмической промышленности Республики Казахстан *Б. Атамкулов*

"СОГЛАСОВАНО"
Председатель Комитета национальной безопасности Республики Казахстан
_____ К. Масимов
"___" _____ 2018 год

Приложение 1
к приказу Министра оборонной
и аэрокосмической промышленности
Республики Казахстан
от 27 июня 2018 года № 105/НҚ

Профили защиты средств антивирусной защиты для рабочих станций и серверов, а также систем обнаружения вторжений уровня сети

Раздел 1. Профиль защиты средств антивирусной защиты для рабочих станций и серверов

Глава 1. Общие положения

1. Настоящий Профиль защиты средств антивирусной защиты для рабочих станций и серверов, разработан в соответствии с подпунктом 18) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации".

2. В настоящем профиле защиты средств антивирусной защиты для рабочих станций и серверов используются следующие основные понятия:

1) объекты информационно-коммуникационной инфраструктуры (далее - ОИКИ) - информационные системы, технологические платформы, аппаратно-программные комплексы, сети телекоммуникаций, а также системы обеспечения бесперебойного функционирования технических средств и информационной безопасности;

2) угроза безопасности информации - совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации;

3) объект оценки (далее - ОО) - подлежащие оценке компоненты ОИКИ с руководствами администратора и пользователя;

4) политика безопасности ОО (далее - ПБО) - совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых ОО;

5) функции безопасности ОО (далее - ФБО) - совокупность всех функций безопасности ОО, направленных на осуществление ПБО;

6) антивирусная защита - защита информации и компонентов ОИКИ от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование "зараженных" объектов, удаление вредоносных компьютерных программ из "зараженных" объектов);

7) средство антивирусной защиты (далее – САВЗ) - программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации;

8) база данных признаков вредоносных компьютерных программ (вирусов) (далее – БД ПКВ) - составная часть САВЗ, содержащая информацию о вредоносных компьютерных программах (вирусах) (сигнатуры), используемая САВЗ для обнаружения вредоносных компьютерных программ (вирусов) и их обработки;

9) администратор безопасности - ответственный за установку, администрирование и эксплуатацию ОО;

10) задание по безопасности (далее – ЗБ) - совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО;

11) профиль защиты (далее – ПЗ) – перечень минимальных требований к безопасности программных и технических средств, являющихся компонентами объектов информатизации;

12) сигнатура - характерные признаки компьютерной вредоносной программы (вируса) (далее – КВ), используемые для ее обнаружения.

3. Основными угрозами, для противостояния которым используются САВЗ, являются угрозы, связанные с внедрением в ОИКИ из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и (или) съемных машинных носителей информации, КВ.

4. В САВЗ реализованы следующие функции безопасности:

1) разграничение доступа к управлению САВЗ;

2) управление работой САВЗ;

3) управление параметрами САВЗ;

4) управление установкой обновлений (актуализации) БД ПКВ САВЗ;

5) аудит безопасности САВЗ;

6) выполнение проверок объектов воздействия;

7) обработка объектов воздействия;

8) сигнализация САВЗ.

5. В среде, в которой САВЗ функционирует, реализованы следующие функции безопасности среды:

1) обеспечение доверенной связи (маршрута) между САВЗ и пользователями;

2) обеспечение доверенного канала получения обновлений САВЗ;

3) обеспечение условий безопасного функционирования;

4) управление атрибутами безопасности.

6. В ПЗ следующие виды требований безопасности, предъявляемые к САВЗ:

1) функциональные требования безопасности (далее - ФТБ);

2) требования доверия к безопасности.

7. ФТБ САВЗ включают:

1) требования к режимам и методам выполнения проверок в целях обнаружения КВ;

2) требования к функциональным возможностям по обновлению БД ПКВ;

3) требования по управлению режимами выполнения функций безопасности САВЗ (работой САВЗ);

4) требования по управлению данными функций безопасности (данными САВЗ);

5) требования по управлению;

6) требования к аудиту функционирования САВЗ.

8. Требования доверия к безопасности САВЗ охватывают следующие основные вопросы:

1) управление конфигурацией;

2) поставка и эксплуатация;

3) разработка;

4) руководства;

5) поддержка жизненного цикла;

6) тестирование;

7) оценка уязвимостей;

8) обновление САВЗ.

9. САВЗ, соответствующие настоящему ПЗ, обеспечивают:

1) выполнения проверок с целью обнаружения зараженных КВ объектов в файловых областях носителей информации;

2) выполнения проверок с целью обнаружения зараженных КВ объектов по команде ;

3) выполнения проверок с целью обнаружения зараженных КВ объектов сигнатурными методами;

4) получения и установки обновлений БД ПКВ без применения средств автоматизации;

5) генерирования записей аудита для событий, подвергаемых аудиту;

6) чтения информации из записей аудита;

7) ограничение доступа к чтению записей аудита;

8) поиск, сортировку, упорядочение данных аудита.

10. САВЗ устанавливаются на рабочие станции и сервера ОИКИ, функционирующие на базе вычислительной сети.

11. Типовая схема применения в ОИКИ САВЗ представлена в приложении 1 к настоящему ПЗ.

Глава 2. Среда безопасности объекта оценки

Параграф 1. Предположения безопасности

12. Предположения относительно предопределенного использования ОО включают в себя:

1) предположение-1.

Доступ ОО ко всем ОИКИ, которые необходимы ОО для реализации своих функциональных возможностей (к контролируемым ОИКИ);

2) предположение-2.

Установка, конфигурирование и управление ОО в соответствии с эксплуатационной документацией;

3) предположение-3.

Совместимость ОО с контролируемыми ресурсами ОИКИ;

4) предположение-4.

Корректная совместная работа САВЗ с САВЗ других производителей в случае их совместного использования в информационной системе;

5) Предположение-5.

Физическая защита элементов ОИКИ, на которых установлен ОО;

6) предположение-6.

Синхронизация по времени между компонентами ОО, а также между ОО и средой его функционирования;

7) предположение-7.

Персонал, ответственный за функционирование ОО, обеспечивает надлежащее функционирование ОО, руководствуясь эксплуатационной документацией.

Параграф 2. Угрозы

13. Угрозы, которым противостоит ОО:

1) угроза-1:

описание угрозы - внедрение КВ в автоматизированные рабочие места ОИКИ при осуществлении информационного взаимодействия с внешними информационно-телекоммуникационными сетями, в том числе сетями международного информационного обмена (сетями связи общего пользования);

источник угрозы - внутренний нарушитель, внешний нарушитель;

способ реализации угрозы - внедрение КВ в ОИКИ при осуществлении информационного обмена;

используемые уязвимости - неполнота комплекса средств защиты информации, применяемые в ОИКИ;

вид информационных ресурсов, потенциально подверженных угрозе - информационные ресурсы ОИКИ, в которой установлен ОО;

нарушаемые свойства безопасности информационных ресурсов - конфиденциальность, целостность, доступность;

возможные последствия реализации угрозы - заражение компьютерными вирусами программно-технических средств вычислительной сети ОИКИ, утечка конфиденциальной информации, нарушение режимов функционирования ОИКИ;

2) угроза-2:

описание угрозы - внедрение КВ в автоматизированные рабочие места ОИКИ со съемных машинных носителей информации;

источник угрозы - внутренний нарушитель;

способ реализации угрозы - внедрение КВ в объекты ОИКИ пользователями со съемных машинных носителей информации;

используемые уязвимости - неполнота комплекса средств защиты информации, применяемые в ОИКИ;

вид информационных ресурсов, потенциально подверженных угрозе - информационные ресурсы ОИКИ, в которой установлен ОО;

нарушаемые свойства безопасности информационных ресурсов - конфиденциальность, целостность, доступность;

возможные последствия реализации угрозы - заражение компьютерными вирусами программно-технических средств вычислительной сети ОИКИ, утечка конфиденциальной информации, нарушение режимов функционирования ОИКИ.

14. Угрозы, которым противостоит среда:

1) угроза среды-1:

описание угрозы - отключение или блокирование САВЗ нарушителями;

источники угрозы - внутренний нарушитель, внешний нарушитель;

способ реализации угрозы - несанкционированный доступ к САВЗ с использованием штатных и нештатных средств;

используемые уязвимости - недостатки процедур разграничения полномочий в ОИКИ, уязвимости технических, программных и программно-технических средств

ОИКИ, которые взаимодействуют с САВЗ и могут влиять на функционирование САВЗ, недостатки механизмов управления доступом, защиты сеансов, физической защиты оборудования в ОИКИ;

вид информационных ресурсов, потенциально подверженных угрозе - данные ФБО;

нарушаемые свойства безопасности информационных ресурсов - целостность, доступность;

возможные последствия реализации угрозы - неэффективность работы САВЗ;

2) угроза среды-2:

описание угрозы - несанкционированное изменение конфигурации САВЗ;

источник угрозы - внутренний нарушитель, внешний нарушитель;

способ реализации угрозы - несанкционированный доступ к конфигурационной информации (настройкам) САВЗ;

используемая уязвимость - недостатки процедур разграничения полномочий в ОИКИ, уязвимости технических, программных и программно-технических средств ОИКИ, которые взаимодействуют с САВЗ и могут влиять на функционирование САВЗ, недостатки механизмов управления доступом, защиты сеансов, физической защиты оборудования в ОИКИ;

вид информационных ресурсов, потенциально подверженные угрозе - настройки программного обеспечения САВЗ;

нарушаемые характеристики безопасности информационных ресурсов – целостность;

возможные последствия реализации угрозы - нарушение режимов функционирования САВЗ, не обнаружение внедрения в ОИКИ КВ;

3) угроза среды-3:

описание угрозы - несанкционированное внесения изменений в логику функционирования САВЗ через механизм обновления БД ПКВ;

источник угрозы - внутренний нарушитель, внешний нарушитель;

способ реализации угрозы - осуществление несанкционированных действий с использованием штатных средств, предоставляемых ОИКИ, а также специализированных инструментальных средств;

используемая уязвимость - недостатки механизмов обеспечения доверенного канала получения обновлений БД ПКВ;

вид информационных ресурсов, потенциально подверженных угрозе - программное обеспечение (далее - ПО) и база данных признаков КВ САВЗ;

нарушаемые свойства безопасности информационных ресурсов -целостность, доступность;

возможные последствия реализации угрозы - нарушение режимов функционирования САВЗ, необнаружение внедрения в ОИКИ КВ. САВЗ следует приведенным ниже правилам политики безопасности организации.

Параграф 3. Политика безопасности организации

15. САВЗ работает по политики безопасности организации:

1) политика безопасности-1.

Механизмы регистрации предоставляют уполномоченным субъектам ОИКИ возможность выборочного ознакомления с информацией о произошедших событиях;

2) политика безопасности-2.

Управление параметрами САВЗ, которые влияют на выполнение функций безопасности САВЗ, осуществляются только уполномоченными субъектами ОИКИ;

3) политика безопасности-3.

Управление со стороны уполномоченных субъектов ОИКИ режимами выполнения функций безопасности САВЗ;

4) политика безопасности-4.

САВЗ защищена от несанкционированного доступа и нарушений в отношении функций и данных САВЗ;

5) политика безопасности-5.

САВЗ обеспечивает выполнение проверок с целью обнаружения зараженных КВ объектов в заданных областях памяти и файлах;

6) политика безопасности-6.

САВЗ обеспечивает возможность установки режимов выполнения проверок с целью обнаружения зараженных КВ объектов;

7) политика безопасности-7.

САВЗ обеспечивать возможность удаления (если удаление технически возможно) кода КВ из зараженных объектов;

8) политика безопасности-8.

САВЗ обеспечивает возможность установки режимов выполнения обновлений БД ПКВ САВЗ.

Глава 3. Цели безопасности

Параграф 1. Цели безопасности для объекта оценки

16. Описание целей безопасности для ОО:

1) цель безопасности-1. Аудит безопасности САВЗ.

САВЗ располагают надлежащими механизмами регистрации и предупреждения о любых событиях, относящихся к возможным нарушениям безопасности. Механизмы регистрации предоставляют уполномоченным субъектам ОИКИ возможность выборочного ознакомления с информацией о произошедших событиях;

2) цель безопасности-2. Управление параметрами САВЗ.

САВЗ обеспечивают возможность управления параметрами САВЗ, которые влияют на выполнение функций безопасности САВЗ, со стороны уполномоченных субъектов ОИКИ;

3) Цель безопасности-3. Управление работой САВЗ.

САВЗ обеспечивают управление со стороны уполномоченных субъектов ОИКИ режимами выполнения функций безопасности САВЗ;

4) цель безопасности-4. Разграничение доступа к управлению САВЗ.

САВЗ обеспечивают разграничение доступа к управлению САВЗ на основе субъектов ОИКИ;

5) цель безопасности-5. Выполнение проверок объектов.

САВЗ обеспечивают выполнение проверок с целью обнаружения зараженных КВ объектов;

6) цель безопасности-6. Режимы выполнения проверок.

САВЗ обеспечивают возможность установки режимов выполнения проверок с целью обнаружения зараженных КВ объектов;

7) цель безопасности-7. Обработка зараженных объектов.

САВЗ обеспечивают возможность удаления (если удаление технически возможно) кода КВ из зараженных объектов;

8) цель безопасности-8. Обновление базы данных.

САВЗ обеспечивают возможность установки режимов выполнения обновлений БД ПКВ САВЗ.

Параграф 2. Цели безопасности для среды объекта оценки

17. Описание целей безопасности для среды функционирования ОО:

1) цель для среды функционирования ОО-1. Доступ к данным ОИКИ.

Обеспечение доступа САВЗ к данным ОИКИ, которые необходимы ОО для реализации своих функциональных возможностей;

2) цель для среды функционирования ОО-2. Эксплуатация ОО.

Установка, конфигурирование и управление САВЗ в соответствии с эксплуатационной документацией;

3) цель для среды функционирования ОО-3. Совместимость.

Совместимость САВЗ с контролируемыми ресурсами ОИКИ;

4) цель для среды функционирования ОО-4. Совместная работа.

Корректная совместная работа САВЗ с САВЗ других производителей в случае их совместного использования в ОИКИ;

5) цель для среды функционирования ОО-5. Физическая защита частей ОО.

Физическая защита программно-технических средств, на которых установлено САВЗ;

6) цель для среды функционирования ОО-6. Синхронизация по времени.

Обеспечение надлежащего источника меток времени и синхронизация по времени между компонентами САВЗ, а также между САВЗ и средой их функционирования;

7) цель для среды функционирования ОО-7. Требования к персоналу.

Персонал, ответственный за функционирование САВЗ, обеспечивают надлежащее функционирование САВЗ, руководствуясь эксплуатационной документацией;

8) цель для среды функционирования ОО-8. Доверенная связь.

Доверенная связь между САВЗ и уполномоченными субъектами ОИКИ (администраторами безопасности);

9) цель для среды функционирования ОО-9. Механизмы аутентификации и идентификации.

Функционирование САВЗ осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности САВЗ;

10) цель для среды функционирования ОО-10. Доверенный канал.

Обеспечение доверенного канала получения обновлений БД ПКВ САВЗ;

11) цель для среды функционирования ОО-11. Защита данных ФБО.

Защищенная область для выполнения функций безопасности САВЗ;

12) цель для среды функционирования ОО-12. Управление атрибутами безопасности.

Управление атрибутами безопасности, связанными с доступом к функциям и данным САВЗ, предоставляться только администраторам САВЗ и ОИКИ.

Глава 4. Обоснование

Параграф 1. Обоснование целей безопасности объекта оценки

18. Цели безопасности:

1) цель безопасности-1.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам Угроза-1, Угроза-2 и реализацией политики безопасности организации Политика безопасности-1, так как обеспечивает надлежащую регистрацию и предупреждение о любых событиях, относящихся к возможным нарушениям безопасности, возможность выборочного ознакомления с информацией о произошедших событиях;

2) цель безопасности-2.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам Угроза-1, Угроза-2 и реализацией политики безопасности организации Политика безопасности-2, так как обеспечивает возможность управления параметрами

САВЗ, которые влияют на выполнение функций безопасности САВЗ, со стороны уполномоченных субъектов ОИКИ;

3) цель безопасности-3.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам Угроза-1, Угроза-2 и реализацией политики безопасности организации Политика безопасности-3, так как обеспечивает управление со стороны уполномоченных субъектов ОИКИ режимами выполнения функций безопасности САВЗ;

4) цель безопасности-4.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе Угроза-2 и реализацией политики безопасности организации Политика безопасности-4, так как обеспечивает разграничение доступа к управлению САВЗ на основе уполномоченных субъектов ОИКИ;

5) цель безопасности-5.

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации Политика безопасности-5, так как обеспечивает выполнение проверок с целью обнаружения зараженных КВ объектов в заданных областях памяти и файлах;

6) цель безопасности-6.

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации Политика безопасности-6, так как обеспечивает возможность установки режимов выполнения проверок с целью обнаружения зараженных КВ объектов;

7) цель безопасности-7.

Достижение этой цели безопасности необходимо в связи с реализацией политики без опасности организации Политика безопасности-7, так как обеспечивает возможность удаления (если удаление технически возможно) кода КВ из зараженных объектов;

8) цель безопасности-8.

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации Политика безопасности-8, так как обеспечивает возможность установки режимов выполнения обновлений БДПКВ САВЗ;

19. Отображение целей безопасности для ОО на угрозы и политику безопасности организации приведено в приложении 2 к настоящему ПЗ.

Параграф 2. Обоснование целей безопасности для среды объекта оценки

20. Отображение целей безопасности для среды на предположения безопасности, политику безопасности и угрозы приведены в приложении 3 к настоящему ПЗ:

1) цель для среды функционирования ОО-1.

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности Предположение-1, так как обеспечивается доступ САВЗ ко всем данным ОИКИ, которые необходимы САВЗ для реализации своих функциональных возможностей;

2) цель для среды функционирования ОО-2.

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности Предположение-2, так как обеспечивается установка, конфигурирование и управление САВЗ в соответствии с эксплуатационной документацией;

3) цель для среды функционирования ОО-3.

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности Предположение-3, так как обеспечивает совместимость САВЗ с контролируемыми информационными ресурсами ОИКИ;

4) цель для среды функционирования ОО-4.

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности Предположение-4, так как обеспечивается возможность корректной совместной работы САВЗ с САВЗ других производителей в случае их совместного использования в информационной системе;

5) цель для среды функционирования ОО-5.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды Угроза для среды-1 и реализацией предположения безопасности Предположение-5, так как обеспечивается физическая защита элементов ОИКИ, на которых установлено САВЗ;

6) цель для среды функционирования ОО-6.

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности Предположение-6, так как обеспечивается синхронизация по времени между компонентами САВЗ, а также между САВЗ и средой его функционирования;

7) цель для среды функционирования ОО-7.

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности Предположение-7, так как персонал, ответственный за функционирование САВЗ, обеспечивает надлежащее функционирование САВЗ, руководствуясь эксплуатационной документацией;

8) цель для среды функционирования ОО-8.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды Угроза для среды-2, так как обеспечивает доверенную связь между САВЗ и уполномоченными субъектами ОИКИ (администраторами безопасности);

9) цель для среды функционирования ОО-9.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды Угроза для среды-1 и Угроза для среды-2, так как обеспечивает функционирование САВЗ в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности САВЗ;

10) цель для среды функционирования ОО-10.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды Угроза для среды-3, так как обеспечивается доверенный канал получения обновлений БД ПКВ САВЗ;

11) цель для среды функционирования ОО-11.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды Угроза для среды-1 и Угроза для среды-2, так как обеспечивается защищенная область для выполнения функций безопасности САВЗ;

12) цель для среды функционирования ОО-12.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды Угроза для среды-1 и Угроза для среды-2, так как обеспечивается предоставления возможности управления атрибутами безопасности, связанными с доступом к функциям и данным ОО, только уполномоченным администраторам САВЗ и ОИКИ.

Раздел 2. Профиль защиты систем обнаружения вторжений уровня сети

Глава 1. Общие положения

1. Настоящий Профиль защиты систем обнаружения вторжений уровня сети разработан в соответствии с подпунктом 18) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации".

2. В настоящем Профиле защиты систем обнаружения вторжений уровня сети используются следующие основные понятия:

1) объекты информационно-коммуникационной инфраструктуры (далее – ОИКИ) - информационные системы, технологические платформы, аппаратно-программные комплексы, сети телекоммуникаций, а также системы обеспечения бесперебойного функционирования технических средств и информационной безопасности;

2) угроза безопасности информации - совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации;

3) система обнаружения вторжений (далее - СОВ) - программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (

носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

4) администратор СОВ - ответственный за установку, администрирование и эксплуатацию ОО;

5) анализатор СОВ - программный или программно-технический компонент СОВ, предназначенный для сбора информации от сенсоров (датчиков) СОВ, ее итогового анализа на предмет обнаружения вторжения (атаки) на контролируемый ОИКИ;

6) данные СОВ - данные, собранные или созданные СОВ в результате выполнения своих функций;

7) датчик (сенсор) СОВ - программный или программно-технический компонент СОВ, предназначенный для сбора и первичного анализа информации (данных) о событиях в контролируемой ОИКИ, а также - передачи этой информации (данных) анализатору СОВ;

8) вторжение (атака) - действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам;

9) объект оценки (далее - ОО) - СОВ уровня сети с руководствами по эксплуатации, подлежащая сертификации (оценке);

10) политика безопасности ОО - совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых ОО;

11) профиль защиты (далее – ПЗ) – перечень минимальных требований к безопасности программных и технических средств, являющихся компонентами объектов информатизации;

12) функции безопасности ОО - совокупность всех функций безопасности ОО, направленных на осуществление политики безопасности объекта оценки (далее - ПБО);

13) сигнатура - характерные признаки вторжения (атаки), используемые для его (ее) обнаружения;

14) задание по безопасности - совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО;

15) база решающих правил (далее - БРП) - составная часть СОВ, содержащая информацию о вторжениях (сигнатуры), на основе которой СОВ принимает решение о наличии вторжения (атаки).

3. СОВ представляет собой элемент системы защиты информации информационных систем, функционирующих на базе вычислительных сетей, и применяется совместно с другими средствами защиты информации от несанкционированного доступа к информации в информационных системах.

4. СОВ обеспечивает обнаружение и (или) блокирование следующих основных угроз безопасности информации, относящихся к вторжениям (атакам):

1) преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена;

2) преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

5. Основными компонентами СОВ являются датчики (сенсоры) и анализаторы.

6. Датчики (сенсоры) собирают информацию о пакетах данных, передаваемых в пределах ОИКИ, в которой (котором) установлены эти датчики. Датчики СОВ уровня сети могут быть реализованы в виде программного обеспечения (ПО), устанавливаемого на стандартные программно-технические платформы, а также в виде программно-технических устройств, подключаемых к ОИКИ. Анализаторы выполняют анализ собранной датчиками информации, генерируют отчеты по результатам анализа и управляют процессами реагирования на выявленные вторжения.

7. Решение об обнаружении вторжения СОВ принимают в соответствии с результатами анализа информации, собираемой датчиками СОВ, с применением базы решающих правил СОВ.

8. В СОВ реализованы следующие функции безопасности:

1) разграничение доступа к управлению СОВ;

2) управление работой СОВ;

3) управление параметрами СОВ;

4) управление установкой обновлений (актуализации) базы решающих правил СОВ;

5) анализ данных СОВ;

6) аудит безопасности СОВ;

7) сбор данных о событиях и активности в контролируемой информационной системе;

8) реагирование СОВ.

9. В среде, в которой СОВ функционирует, реализованы следующие функции безопасности среды:

1) обеспечение доверенного маршрута;

2) обеспечение доверенного канала;

3) обеспечение условий безопасного функционирования;

4) управление атрибутами безопасности.

10. Функции безопасности СОВ обладают составом функциональных возможностей , обеспечивающих реализацию этих функций.

11. ФТБ СОВ включают:

1) требования по осуществлению сбора данных СОВ;

2) требования к анализу данных СОВ;

3) требования к реагированию СОВ;

4) требования к средствам обновления базы решающих правил СОВ;

5) требования по защите СОВ;

6) требования по управлению режимами выполнения функций безопасности (работой СОВ);

7) требования по управлению данными функций безопасности (данными СОВ);

8) требования по управлению субъектов;

9) требования к средствам администрирования СОВ;

10) требования к аудиту функционирования СОВ.

12. Требования доверия к безопасности СОВ, в ПЗ, охватывают следующие вопросы:

1) управление конфигурацией; поставка и эксплуатация; разработка; руководства;

2) поддержка жизненного цикла;

3) тестирование;

4) оценка уязвимостей;

5) обновление базы решающих правил.

13. СОВ, соответствующие настоящему ПЗ, обеспечивают:

1) возможность сбора информации о сетевом трафике;

2) возможность выполнения анализа собранных данных СОВ о сетевом трафике в режиме, близком к реальному масштабу времени, и по результатам анализа фиксировать информацию о дате и времени, результате анализа, идентификаторе источника данных, протоколе, используемом для проведения вторжения;

3) возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием сигнатурного и эвристических методов;

4) возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика на заданном уровне эвристического анализа;

5) возможность обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня базовой эталонной модели взаимосвязи открытых систем;

6) возможность фиксации факта обнаружения вторжений или нарушений безопасности в журналах аудита;

7) уведомление администратора СОВ об обнаруженных вторжениях по отношению к контролируемым узлам ОИКИ и нарушениях безопасности с помощью отображения соответствующего сообщения на консоли управления;

8) возможность автоматизированного обновления базы решающих правил;

9) возможность тестирования (самотестирования) функций безопасности СОВ (контроль целостности исполняемого кода СОВ);

10) возможность со стороны уполномоченных администраторов управлять режимом выполнения функций безопасности СОВ;

11) возможность со стороны уполномоченных администраторов управлять данными СОВ;

12) поддержка для СОВ и их ассоциации с конкретными администраторами СОВ и пользователями ИС;

13) возможность администрирования СОВ;

14) возможность генерации записей аудита для событий, потенциально подвергаемых аудиту;

15) возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;

16) возможность предоставлять возможность читать информацию из записей аудита ;

17) ограничение доступа к чтению записей аудита;

18) поиск, сортировка, упорядочение данных аудита.

14. В общем виде архитектура СОВ включает следующие компоненты:

1) датчики (сенсоры) СОВ, предназначенные для сбора необходимой информации о функционировании ОИКИ;

2) анализаторы СОВ, выполняющие анализ данных, собранных датчиками, с целью обнаружения вторжений;

3) хранилище, обеспечивающее хранение информации о событиях, зафиксированных вторжениях, а также сигнатуры вторжений и другую информацию базы решающих правил, на основании которой принимается решение о наличии вторжения;

4) консоль управления компонентами СОВ, позволяющая администратору безопасности конфигурировать СОВ, наблюдать за состоянием защищаемой ОИКИ и СОВ, просматривать выявленные анализатором инциденты.

15. Основными компонентами СОВ являются датчик(и) и анализатор(ы) СОВ. Датчики собирают информацию о сетевом трафике, поступающем в ОИКИ, осуществляют первичный анализ и направляют эту информацию (данные) анализатору. Анализатор выполняет анализ собранных данных, уведомляют администраторов СОВ об обнаруженных вторжениях, выполняют другие действия по реагированию, генерируют отчеты на основе собранной информации (данных).

16. Датчики уровня сети могут устанавливаться в разрыв канала связи контролируемого сегмента ИС; путем подключения к портам сетевого оборудования ОИКИ, а также быть интегрированными в межсетевые экраны или в коммуникационное оборудование ОИКИ.

17. Анализатор обладает функциональными возможностями:

1) принимать данные от датчиков;

2) обрабатывать данные с целью выявления вторжений;

3) реагировать на выявленные вторжения.

18. Реагирование может включать создание отчетов, отображение сообщения на консоли управления и иные возможности по реагированию.

19. Решение об обнаружении вторжения СОВ принимает в соответствии с результатами анализа информации, собираемой сенсорами СОВ, с применением базы решающих правил СОВ.

20. Администрирование СОВ может выполняться удаленным или локальным способами. Локальное администрирование осуществляется непосредственно с того узла, где установлен компонент СОВ, а удаленное - посредством команд, посылаемых по каналам связи.

21. Все компоненты СОВ обладают функциональными возможностями:

1) осуществлять защиту (совместно с механизмами среды функционирования) собственной программной и информационной части от вмешательства;

2) допускать настройку своих параметров со стороны администратора безопасности

.

Типовая схема применения в ОИКИ СОВ уровня сети представлена в приложении 4 к настоящему ПЗ.

22. Функционирование СОВ подчинено политике безопасности СОВ, отраженной в функциональных требованиях безопасности СОВ.

Глава 2. Среда безопасности объекта оценки

Параграф 1. Предположения безопасности

23. Предположения относительно предопределенного использования СОВ включают в себя:

1) предположение-1.

Обеспечение доступа СОВ ко всем объектам ОИКИ, для реализации своих функциональных возможностей (к контролируемым объектам ОИКИ);

2) предположение-2.

Установка, конфигурирование и управление СОВ в соответствии с эксплуатационной документацией;

3) предположение-3.

Совместимость СОВ с элементами ОИКИ, контроль которой он осуществляет;

4) предположение-4.

Физическая защита элементов ОИКИ, на которых установлены компоненты СОВ, критически важные с точки зрения осуществления политики безопасности СОВ;

5) предположение-5.

Синхронизация по времени между компонентами СОВ, а также между СОВ и средой ее функционирования;

6) предположение-6.

Персонал, ответственный за функционирование СОВ, обеспечивают надлежащее функционирование СОВ, руководствуясь эксплуатационной документацией.

Параграф 2. Угрозы

24. Угрозы, которым противостоит ОО:

1) угроза-1:

описание угрозы - преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена;

источник угрозы - внешние нарушители;

способ реализации угрозы - обход механизмов безопасности ОИКИ с использованием штатных средств, предоставляемых ОИКИ, а также специализированных инструментальных средств;

используемые уязвимости - недостатки средств защиты информации, применяемые в ОИКИ;

вид информационных ресурсов, потенциально подверженных угрозе - данные пользователей, конфигурационные данные, другие ресурсы ОИКИ;

нарушаемое свойство безопасности информационных ресурсов -целостность, доступность, конфиденциальность;

возможные последствия реализации угрозы - нарушения режимов функционирования ОИКИ, снижение уровня защиты ОИКИ;

2) угроза-2:

описание угрозы - преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе;

источник угрозы - внутренние нарушители;

способ реализации угрозы - обход механизмов безопасности ОИКИ с использованием штатных средств, предоставляемых ОИКИ, а также специализированных инструментальных средств;

используемые уязвимости - недостатки средств защиты информации, применяемые в ОИКИ;

вид информационных ресурсов, потенциально подверженных угрозе - данные пользователей, конфигурационные данные, другие ресурсы ОИКИ;

нарушаемое свойство безопасности информационных ресурсов -целостность, доступность, конфиденциальность;

возможные последствия реализации угрозы - нарушения режимов функционирования ОИКИ, снижение уровня защиты ОИКИ.

25. Угрозы, которым противостоит среда функционирования СОВ:

1) угроза среды-1:

описание угрозы - нарушение целостности данных, собранных или созданных СОВ (данных СОВ);

источник угрозы - внутренний нарушитель, внешний нарушитель;

способ реализации угрозы - несанкционированный доступ к данным СОВ с использованием штатных и нештатных средств;

используемая уязвимость - недостатки механизмов управления доступом, защиты сеансов, физической защиты оборудования ОИКИ, недостатки механизмов защиты журналов аудита СОВ;

вид информационных ресурсов, потенциально подверженных угрозе - данные СОВ;

нарушаемые свойства безопасности информационных ресурсов - целостность, доступность;

возможные последствия реализации угрозы - невозможность использования собранной СОВ информации о возможных вторжениях (атаках) для принятия решений о реагировании;

2) угроза среды-2:

описание угрозы - отключение или блокирование нарушителем компонентов СОВ;

источник угрозы - внутренний нарушитель, внешний нарушитель;

способ реализации угрозы - несанкционированный доступ к компонентам СОВ;

используемая уязвимость - недостатки процедур разграничения полномочий в ОИКИ, уязвимости СОВ, внесенные на этапах проектирования и разработки, недостатки контроля программной среды ОИКИ;

вид информационных ресурсов, потенциально подверженные угрозе - ПО и база решающих правил СОВ;

нарушаемые свойства безопасности информационных ресурсов - целостность, доступность;

возможные последствия реализации угрозы - нарушение режимов функционирования СОВ, не обнаружение реализуемых по отношению к ОИКИ вторжений (атак);

3) угроза среды-3:

описание угрозы - несанкционированное изменение конфигурации СОВ;

источник угрозы - внутренний нарушитель, внешний нарушитель;

способ реализации угрозы - несанкционированный доступ к конфигурационной информации (настройкам) СОВ;

используемая уязвимость - недостатки процедур разграничения полномочий в ОИКИ, уязвимости технических, программных и программно-технических средств ОИКИ, которые взаимодействуют с СОВ и могут влиять на функционирование СОВ, недостатки механизмов управления доступом, защиты сеансов, физической защиты оборудования в ОИКИ;

вид информационных ресурсов, потенциально подверженные угрозе - настройки программного обеспечения СОВ;

нарушаемые характеристики безопасности активов - целостность;

возможные последствия реализации угрозы - нарушение режимов функционирования СОВ, не обнаружение реализуемых по отношению к ОИКИ вторжений (атак);

4) угроза среды-4:

описание угрозы - несанкционированное внесение изменений в логику функционирования СОВ через механизм обновления базы решающих правил;

источник угрозы - внутренние нарушители, внешние нарушители;

способ реализации угрозы - осуществление несанкционированных действий с использованием штатных средств, предоставляемых ОИКИ, а также специализированных инструментальных средств;

используемая уязвимость - недостатки механизмов обеспечения доверенного канала получения обновлений базы решающих правил СОВ;

вид информационных ресурсов, потенциально подверженных угрозе - ПО и база решающих правил СОВ;

нарушаемые свойства безопасности информационных ресурсов -целостность, доступность;

возможные последствия реализации угрозы - нарушение режимов функционирования СОВ, необнаружение реализуемых по отношению к ОИКИ вторжений (атак), невозможность использования собранной СОВ информации о возможных вторжениях (атаках) для принятия решений о реагировании.

Параграф 3. Политика безопасности организации

26. СОВ следует приведенным ниже правилам политики безопасности организации:

1) политика безопасности-1.

Управление параметрами СОВ, которые влияют на выполнение функций безопасности СОВ, осуществляться только администраторами СОВ;

2) политика безопасности-2.

ОО осуществляет сбор информации о сетевом трафике;

3) политика безопасности-3.

Аналитическая обработка собранных СОВ данных о функционировании контролируемой ОИКИ заданными методами с целью вынесения решения об обнаружении вторжения;

4) политика безопасности-4.

Реагирование СОВ на выявленные вторжения;

5) политика безопасности-5.

Управление со стороны уполномоченных администраторов СОВ режимами выполнения функций безопасности СОВ;

6) политика безопасности-6.

ОО защищен от несанкционированного доступа и нарушений в отношении функций и данных СОВ;

7) политика безопасности-7.

Регистрация и учет выполнения функций безопасности СОВ;

8) политика безопасности-8.

Контроль целостности программного кода СОВ;

9) политика безопасности-9.

ОО имеет интерфейс администрирования;

10) политика безопасности-10.

ОО имеет возможность управления режимами получения и установки обновлений (актуализации) базы решающих правил (далее - БРП) СОВ.

Глава 3. Цели безопасности

Параграф 1. Цели безопасности для объекта оценки

27. Описание целей безопасности для СОВ:

1) цель безопасности- 1. Управление параметрами СОВ.

СОВ обеспечивает возможность управления параметрами СОВ (правилами в БРП СОВ, другими данными СОВ), которые влияют на выполнение функций безопасности СОВ, со стороны уполномоченных администраторов СОВ;

2) цель безопасности-2. Сбор данных о событиях и активности в контролируемой ОИКИ.

СОВ осуществляет сбор информации о передаче сетевого трафика;

3) цель безопасности-3. Анализ данных СОВ.

СОВ осуществляет аналитическую обработку собранных СОВ данных о функционировании контролируемой ОИКИ заданными методами с целью вынесения решения об обнаружении вторжения;

4) цель безопасности-4. Реагирование СОВ.

СОВ осуществляет реагирование на выявленные вторжения;

5) цель безопасности-5. Управление работой СОВ.

СОВ обеспечивает управление со стороны уполномоченных администраторов СОВ режимами выполнения функций безопасности СОВ;

6) цель безопасности-6. Разграничение доступа к управлению СОВ.

СОВ обеспечивает разграничение доступа к управлению СОВ на основе администраторов СОВ;

7) цель безопасности-7. Аудит безопасности СОВ.

СОВ обеспечивает регистрацию и учет выполнения функций безопасности СОВ;

8) цель безопасности-8. Контроль целостности СОВ.

СОВ обеспечивает контроль целостности программного кода СОВ;

9) цель безопасности-9. Интерфейс СОВ.

СОВ предоставляет администратору СОВ интерфейс администрирования;

10) цель безопасности-10. Управление установкой обновлений (актуализации) БРП СОВ.

СОВ обеспечивает управление режимами получения и установки обновлений (актуализации) БРП СОВ.

Параграф 2. Цели безопасности для среды объекта оценки

28. Описание целей безопасности для среды функционирования СОВ:

1) цель для среды функционирования ОО-1. Доступ к данным ОИКИ.

Обеспечение доступа СОВ ко всем объектам ОИКИ, которые необходимы СОВ для реализации своих функциональных возможностей (к контролируемым объектам ОИКИ);

2) цель для среды функционирования ОО-2. Эксплуатация СОВ.

Установка, конфигурирование и управление СОВ в соответствии с эксплуатационной документацией;

3) цель для среды функционирования ОО-3. Совместимость.

Совместимость СОВ с элементами ОИКИ, контроль которой он осуществляет;

4) цель для среды функционирования ОО-4. Физическая защита частей СОВ.

Физическая защита элементов ОИКИ, на которых установлены компоненты СОВ, критически важные с точки зрения осуществления политики безопасности СОВ;

5) цель для среды функционирования ОО-5. Доверенная связь.

Доверенная связь (маршрут) между СОВ и администраторами СОВ;

6) цель для среды функционирования ОО-6. Механизмы аутентификации и идентификации.

Функционирование СОВ осуществляется в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов СОВ;

7) цель для среды функционирования ОО-7. Доверенный канал.

Обеспечение доверенного канала получения обновлений БРП СОВ;

8) цель для среды функционирования ОО-8. Защита данных ФБО.

Защищенная область для выполнения функций безопасности СОВ;

9) цель для среды функционирования ОО-9. Синхронизация по времени.

Источник меток времени и синхронизация по времени между компонентами СОВ, а также между СОВ и средой ее функционирования;

10) цель для среды функционирования ОО-10. Хранение данных аудита.

Защита журнала аудита от несанкционированного изменения и удаления, а также возможность управления событиями, потенциально приводящими к переполнению областей хранения данных аудита;

11) цель для среды функционирования ОО-11. Управление атрибутами безопасности.

Возможность управления атрибутами безопасности компонентов СОВ и контролируемых объектов ОИКИ предоставляться только уполномоченным администраторам СОВ и ОИКИ;

12) цель для среды функционирования ОО-12. Требования к персоналу.

Персонал, ответственный за функционирование ОО, обеспечивают надлежащее функционирование ОО, руководствуясь эксплуатационной документацией.

Глава 4. Обоснование

Параграф 1. Обоснование целей безопасности объекта оценки

29. Отображение целей безопасности для ОО на угрозы и политику безопасности организации приведены в приложении 5 к настоящему ПЗ:

1) цель безопасности-1.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам Угроза-1 и Угроза-2, а также реализацией политики безопасности Политика безопасности-1, так как обеспечивает возможность управления параметрами СОВ (правилами в БРП СОВ, другими данными СОВ), которые влияют на выполнение функций безопасности СОВ, со стороны уполномоченных администраторов СОВ;

2) цель безопасности-2.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам Угроза-1 и Угроза-2, а также реализацией политики безопасности Политика безопасности-2, так как обеспечивает сбор информации о передаче сетевого трафика;

3) цель безопасности-3.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам Угроза-1 и Угроза-2, а также реализацией политики безопасности Политика

безопасности-3, так как обеспечивает осуществление аналитической обработки собранных СОВ данных о функционировании контролируемой ОИКИ заданными методами с целью вынесения решения об обнаружении вторжения;

4) цель безопасности-4.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам Угроза-1 и Угроза-2, а также реализацией политики безопасности Политика безопасности-4, так как обеспечивает осуществление реагирования на выявленные вторжения;

5) цель безопасности-5.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам Угроза-1 и Угроза-2, а также реализацией политики безопасности Политика безопасности-5, так как обеспечивает управление со стороны уполномоченных администраторов СОВ режимами выполнения функций безопасности СОВ;

6) цель безопасности-6.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам Угроза-1 и Угроза-2, а также реализацией политики безопасности Политика безопасности-6, так как обеспечивает разграничение доступа к управлению СОВ на основе администраторов СОВ.

7) цель безопасности-7.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам Угроза-1 и Угроза-2, а также реализацией политики безопасности Политика безопасности-7, так как обеспечивает регистрацию и учет выполнения функций безопасности СОВ;

8) цель безопасности-8.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам Угроза-1 и Угроза-2, а также реализацией политики безопасности Политика безопасности-8, так как обеспечивает контроль целостности программного кода;

9) цель безопасности-9.

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности Политика безопасности-9, так как обеспечивает наличие интерфейса администрирования;

10) цель безопасности-10.

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности Политика безопасности-10, так как возможность управления режимами получения и установки обновлений (актуализации) БРП СОВ.

Параграф 2. Обоснование целей безопасности для среды объекта оценки

30. Отображение целей безопасности на предположения безопасности организации приведены в приложении 6 к настоящему ПЗ, отображение целей безопасности на угрозы среды безопасности организации приведены в приложении 7 к настоящему ПЗ:

1) цель для среды функционирования ОО-1.

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности Предположение-1, так как обеспечивает доступ СОВ ко всем объектам ОИКИ, которые необходимы ОО для реализации своих функциональных возможностей (к контролируемым ОИКИ);

2) цель для среды функционирования ОО-2.

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности Предположение-2, так как обеспечивает установку, конфигурирование и управление СОВ в соответствии с эксплуатационной документацией;

3) цель для среды функционирования ОО-3.

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности Предположение-3, так как обеспечивает совместимость СОВ с элементами ОИКИ, контроль которой он осуществляет;

4) цель для среды функционирования ОО-4.

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности Предположение-4 и противостояния угрозе для среды Угроза для среды-3, так как обеспечивает физическую защиту элементов ОИКИ, на которых установлены компоненты СОВ, критически важные с точки зрения осуществления политики безопасности СОВ;

5) цель для среды функционирования ОО-5.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды Угроза для среды-2, так как обеспечивает доверенную связь (маршрут) между СОВ и администраторами СОВ;

6) цель для среды функционирования ОО-6.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды Угрозы для среды-1, 2, 3, так как обеспечивает функционирование СОВ в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов СОВ;

7) цель для среды функционирования ОО-7.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды Угроза для среды-4, так как обеспечивает получение обновлений БРП СОВ по доверенному каналу;

8) цель для среды функционирования ОО-8.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды Угрозы для среды-1, 2, 3, так как обеспечивается защищенная область для выполнения функций безопасности СОВ;

9) цель для среды функционирования ОО-9.

Достижение этой цели безопасности необходимо в связи с реализацией предположения Предположение-5, так как обеспечивается предоставление надлежащего источника меток времени и синхронизация по времени между компонентами СОВ, а также между СОВ и средой их функционирования;

10) цель для среды функционирования ОО-10.

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды Угроза для среды-1, так как обеспечивается защита журнала аудита от несанкционированного изменения и удаления, а также возможность управления событиями, потенциально приводящими к переполнению областей хранения данных аудита;

11) цель для среды функционирования ОО-11.

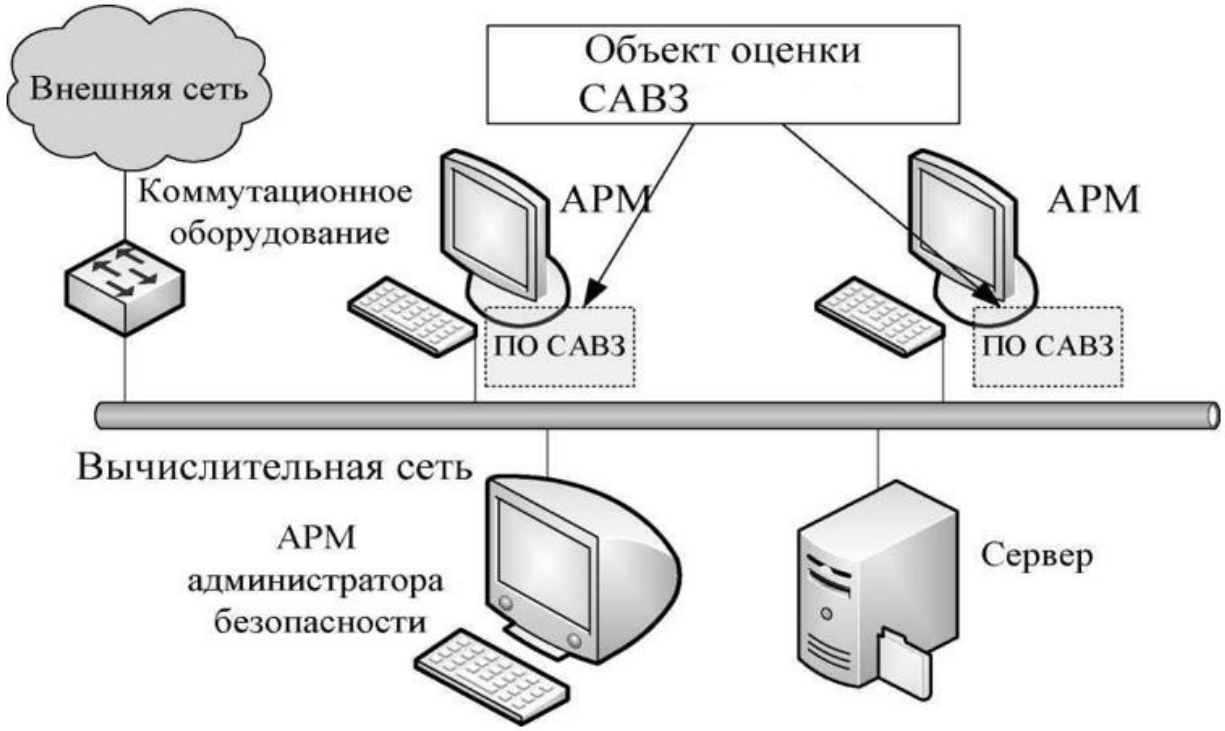
Достижение этой цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды Угрозы для среды-2, 3, так как обеспечивается предоставления возможности управления атрибутами безопасности компонентов СОВ и контролируемых ОИКИ только уполномоченным администраторам СОВ и ОИКИ;

12) цель для среды функционирования ОО-12.

Достижение этой цели безопасности необходимо в связи с реализацией предположения Предположение-5, так как обеспечивает исполнение обязанностей персоналом, ответственным за функционирование СОВ, руководствуясь эксплуатационной документацией.

Приложение 1
к профилям защиты средств
антивирусной защиты для
рабочих станций и серверов, а
также систем обнаружения
вторжений уровня сети

Типовая схема объекта информационно-коммуникационной инфраструктуры, в которой применяется средство антивирусной защиты



Приложение 2
к профилям защиты средств
антивирусной защиты для
рабочих станций и серверов, а
также систем обнаружения
вторжений уровня сети

Отображение целей безопасности для объекта оценки на угрозы и политику безопасности организации

	Цель безопасности -1	Цель безопасности -2	Цель безопасности -3	Цель безопасности -4	Цель безопасности -5	Цель безопасности -6	Цель безопасности -7	Цель безопасно -8
Угроза-1	X	X	X					
Угроза-2	X	X	X	X				
Политика безопасности -1	X							
Политика безопасности -2		X						
Политика безопасности -3			X					
Политика безопасности -4				X				

Политика безопасности -5					X			
Политика безопасности -6						X		
Политика безопасности -7							X	
Политика безопасности -8								X

Приложение 3
к профилям защиты средств антивирусной защиты для рабочих станций и серверов, а также систем обнаружения вторжений уровня сети

Отображение целей безопасности для среды на предположения безопасности, политики безопасности и угрозы

	Цель для среды функционирования ОО-1	Цель для среды функционирования ОО-2	Цель для среды функционирования ОО-3	Цель для среды функционирования ОО-4	Цель для среды функционирования ОО-5	Цель функц ОО-6
Предположение -1	X					
Предположение -2		X				
Предположение -3			X			
Предположение -4				X		
Предположение -5					X	
Предположение -6						X
Предположение -7						
Угроза среды-1					X	
Угроза среды-2						
Угроза среды-3						

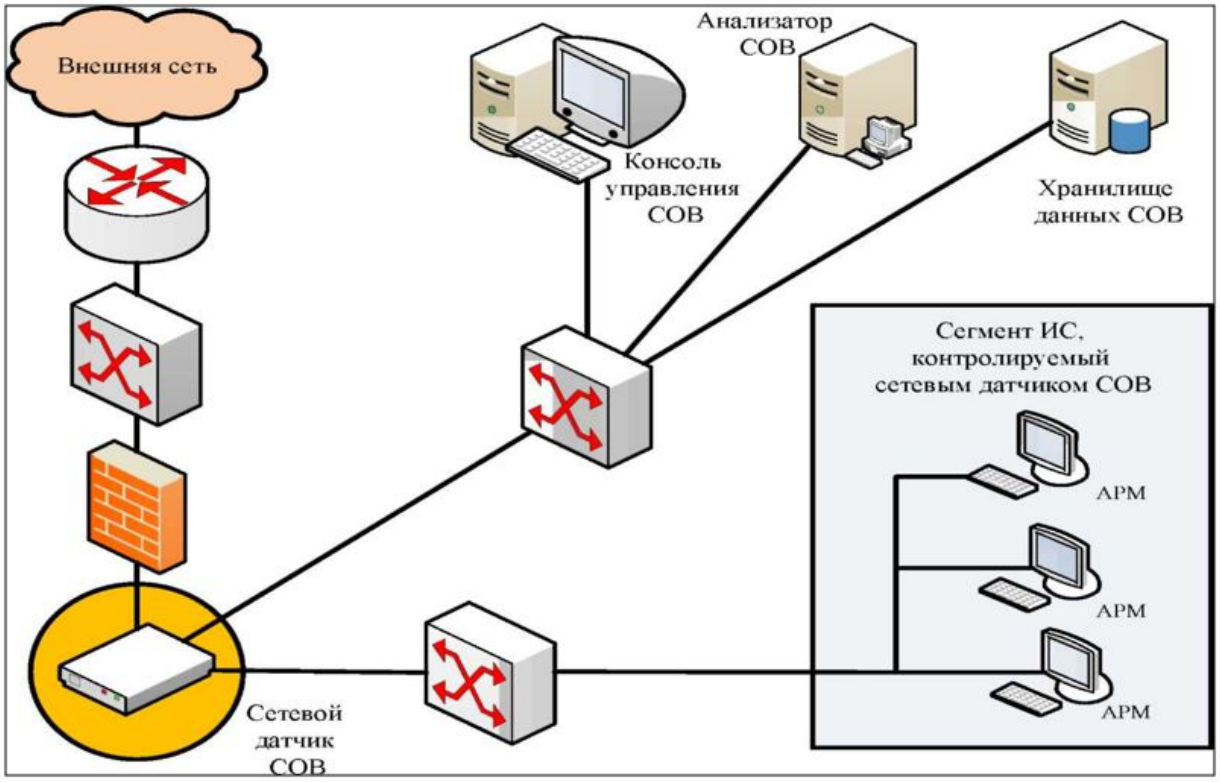
продолжение таблицы

Цель для среды функционирования ОО-10	Цель для среды функционирования ОО-11	Цель для среды функционирования ОО-12

		x
	x	x
	x	x
x		

Приложение 4
к профилям защиты средств
антивирусной защиты для
рабочих станций и серверов, а
также систем обнаружения
вторжений уровня сети

Типовая схема применения в объектах информационно-коммуникационной инфраструктуры система обнаружения вторжений уровня сети



Приложение 5
к профилям защиты средств
антивирусной защиты для
рабочих станций и серверов, а
также систем обнаружения
вторжений уровня сети

Отображение целей безопасности для объекта оценки на угрозы и политику безопасности организации.

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасно-8
Угроза-1	X	X	X	X	X	X	X	X
Угроза-2	X	X	X	X	X	X	X	X
Политика безопасности-1	X							
Политика безопасности-2		X						
Политика безопасности-3			X					
Политика безопасности-4				X				
Политика безопасности-5					X			
Политика безопасности-6						X		
Политика безопасности-7							X	
Политика безопасности-8								X
Политика безопасности-9								
Политика безопасности-10								

Приложение 6
к профилям защиты средств
антивирусной защиты для
рабочих станций и серверов, а
также систем обнаружения
вторжений уровня сети

Отображение целей безопасности для среды на предположения безопасности организации.

	Цель для среды функционирования ОО-1	Цель для среды функционирования ОО-2	Цель для среды функционирования ОО-3	Цель для среды функционирования ОО-4	Цель для среды функционирования ОО-5	Цель функц ОО-6
Предположение -1	X					
Предположение -2		X				
Предположение -3			X			
Предположение -4				X		
Предположение -5						
Предположение -6						

продолжение таблицы

Цель для среды функционирования ОО-9	Цель для среды функционирования ОО-10	Цель для среды функционирования ОО-11	Цель для среды функционирования ОО-12
x			
			x

Приложение 7
к профилям защиты средств
антивирусной защиты для
рабочих станций и серверов, а
также систем обнаружения
вторжений уровня сети

Отображение целей безопасности для среды на угрозы среды безопасности организации.

	Цель для среды функционирования ОО-1	Цель для среды функционирования ОО-2	Цель для среды функционирования ОО-3	Цель для среды функционирования ОО-4	Цель для среды функционирования ОО-5	Цель для сре функционирова ОО-6
Угроза среды-1						X
Угроза среды-2					X	X
Угроза среды-3				X		X

Угроза среды-4						

продолжение таблицы

Цель для среды функционирования ОО-10	Цель для среды функционирования ОО-11	Цель для среды функционирования ОО-12
x		
	x	
	x	

Приложение 2
к приказу Министра оборонной
и аэрокосмической промышленности
Республики Казахстан
от 27 июня 2018 года № 105/НҚ

Методика разработки профилей защиты

Глава 1. Общие положения

1. Настоящая Методика разработки профилей защиты (далее – Методика) разработана в соответствии с подпунктом 18) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации".

2. Методика предназначена для разработки профилей защиты объектов информационно-коммуникационной инфраструктуры.

3. В настоящей Методике используются термины и определения:

1) объекты информационно-коммуникационной инфраструктуры (далее – ОИКИ) – информационные системы, технологические платформы, аппаратно-программные комплексы, сети телекоммуникаций, а также системы обеспечения бесперебойного функционирования технических средств и информационной безопасности;

2) информационно-коммуникационная инфраструктура – совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

3) объект оценки (далее – ОО) – подлежащие оценке компоненты ОИКИ с руководствами администратора и пользователя;

4) доверие к безопасности - основание для уверенности в том, что компоненты ОИКИ отвечают своим целям безопасности;

5) профиль защиты (далее – ПЗ) – перечень минимальных требований к безопасности программных и технических средств, являющихся компонентами объектов информатизации;

6) задание по безопасности – совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОИКИ;

7) политика безопасности ОО - совокупность правил, регулирующих управление активами, их защиту и распределение в пределах ОИКИ;

8) политика безопасности организации - одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности;

9) функция безопасности - функциональные возможности части или частей ОИКИ, обеспечивающие выполнение подмножества взаимосвязанных правил политика безопасности ОО;

10) угроза безопасности (далее – угроза) - совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба ОИКИ или его собственнику;

11) цель безопасности - намерение противостоять установленным угрозам и (или) удовлетворять установленной политике безопасности организации и предположениям.

Глава 2. Требования к профилям защиты

4. ПЗ представляет собой типовой (стандартизованный) набор требований безопасности, которым удовлетворяет классификационная категория компонентов ОИКИ.

5. ПЗ состоит из:

1) описания потребностей пользователей компонентов ОИКИ в обеспечении безопасности;

2) описания политики безопасности организации и среды безопасности компонентов ОИКИ с учетом возможных угроз, порождаемых ей;

3) целей безопасности компонентов ОИКИ, основанные на описании их среды безопасности, а также меры для еҰ обеспечения;

4) функциональных требований безопасности и требования доверия к безопасности компонентов ОИКИ, направленные на решение проблемы их безопасности;

5) описания проблем безопасности (в терминах угроз, предположений и положений политики безопасности) и их решений;

6) обоснования достаточности функциональных требований безопасности и требований доверия к безопасности, представленных в ПЗ, для удовлетворения потребностей пользователей компонентов ОИКИ в их безопасности.

Глава 3. Структура и содержание профиля защиты

6. Профиль защиты содержит следующие главы:

1) Общие положения;

2) Среда безопасности объекта оценки;

3) Цели безопасности;

4) Обоснование.

7. В главе "Общие положения" описываются данные о ПЗ, идентифицируется ПЗ и дается его аннотация в форме, наиболее подходящей для включения в каталоги и описание объекта оценки.

8. В главу "Среда безопасности объекта оценки" включается описание аспектов среды безопасности компонента ОИКИ (представляющего собой ОО), в которой предполагается его использование, а также способ использования данного компонента ОИКИ.

Данная глава содержит параграфы:

1) предположения безопасности (предположения о предназначении компонента ОИКИ и о его среде эксплуатации);

2) угрозы" (угрозы безопасному функционированию компонента ОИКИ);

3) политика безопасности организации (политика безопасности организации, которой удовлетворяет компонент ОИКИ).

9. В главу "Цели безопасности" включается описание целей безопасности ОО (сформулированные решения по противостоянию угрозам безопасному функционированию компонента ОИКИ) и целей безопасности для среды ОО (сформулированные решения по противостоянию угрозам безопасности для среды компонента ОИКИ).

Данная глава содержит параграфы:

1) цели безопасности для объекта оценки;

2) цели безопасности для среды объекта оценки.

10. В главу "Обоснование" включается логическое обоснование целей безопасности и требований безопасности, в том числе, что:

функциональные требования и требования доверия к безопасности для компонента ОИКИ и его среды соответствуют целям безопасности;

требования безопасности не противоречат друг другу;

выбор требований безопасности является обоснованным;

функции компонента ОИКИ согласуются с его целями безопасности.

Данная глава содержит параграфы:

1) Обоснование целей безопасности объекта оценки;

2) Обоснование целей безопасности для среды объекта оценки.