О внесении изменений в приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 27 июня 2018 года № 105/НҚ "Об утверждении профилей защиты и методики разработки профилей защиты"

Приказ Заместителя Премьер-Министра – Министра искусственного интеллекта и цифрового развития Республики Казахстан от 3 июля 2026 года № 380/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 7 июля 2026 года № 39239

Примечание ИЗПИ!

Вводится в действие с 12.07.2026

ПРИКАЗЫВАЮ:

1. Внести в приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 27 июня 2018 года № 105/НҚ "Об утверждении профилей защиты и методики разработки профилей защиты" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 17247) следующие изменения:

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 20) статьи 7-1 Закона Республики Казахстан "О кибербезопасности" **ПРИКАЗЫВАЮ:**"

подпункт 1) пункта 1 изложить в следующей редакции:

"1) Профили защиты согласно приложению 1 к настоящему приказу;";

приложение 1, утвержденное указанным приказом, изложить в новой редакции согласно приложению 1 к настоящему приказу;

приложение 2, утвержденное указанным приказом, изложить в новой редакции согласно приложению 2 к настоящему приказу.

2. Комитету по информационной безопасности Министерства искусственного интеллекта и цифрового развития Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

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

2) размещение настоящего приказа на интернет-ресурсе Министерства искусственного интеллекта и цифрового развития Республики Казахстан после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства искусственного интеллекта и цифрового

развития Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1) и 2) настоящего пункта.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра искусственного интеллекта и цифрового развития Республики Казахстан.

4. Настоящий приказ вводится в действие с 12 июля 2026 года и подлежит официальному опубликованию.

Заместитель Премьер-Министра
– Министр искусственного интеллекта
и цифрового развития
Республики Казахстан *Ж. Мадиев*

Приложение 1 к приказу
Заместитель Премьер-Министра
– Министр искусственного
интеллекта
и цифрового развития
Республики Казахстан
от 3 июля 2026 года
№ 380/НҚ

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

Профили защиты

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

Глава 1. Общие положения

1. Настоящие Профили защиты разработаны в соответствии с подпунктом 20) статьи 7-1 Закона Республики Казахстан "О кибербезопасности".

2. В настоящих профилях защиты используются следующие понятия:

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

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

3) система обнаружения вторжений (далее - СОВ) - программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в цифровой 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 ОЦИ;

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 ОЦИ, а также - передачи этой информации (данных) анализатору СОВ;

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

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

10) антивирусная защита - защита информации и компонентов ОЦИ от вредоносных компьютерных программ (вирусов) (обнаружение, блокирование, изолирование, удаление вредоносных компьютерных программ);

11) 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;

12) 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;

13) угроза кибербезопасности (далее – угроза) - совокупность условий и факторов, создающих предпосылки к возникновению инцидента кибербезопасности;

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

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

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

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

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

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

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

21) объекты цифровой инфраструктуры (далее – ОЦИ) – совокупность материальных, технических и технологических средств, обеспечивающих размещение и среду функционирования цифровых объектов;

22) цифровая инфраструктура – совокупность объектов цифровой инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования цифровых ресурсов и предоставления доступа к ним;

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

Главы 2. Минимальные требования к безопасности программных и технических средств, являющихся компонентами цифровых объектов

3. Минимальные требования к безопасности программных и технических средств, являющихся компонентами цифровых объектов, предъявляемых САВЗ:

1) функциональные требования безопасности (далее - ФТБ);

2) требования доверия к безопасности.

4. 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.

5. 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.

6. САВЗ, соответствующие настоящему ПЗ, обеспечивают:

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

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

3) выполнения проверок с целью обнаружения 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.

7. САВЗ устанавливаются на рабочие станции и сервера ОЦИ, функционирующие на базе вычислительной сети.

8. Типовая схема ОЦИ, в которой применяется средство антивирусной защиты представлена в приложении 1 к настоящему ПЗ.

Глава 3. Среда безопасности объекта оценки

Параграф 1. Предположения безопасности

9. Предположения относительно предопределенного использования ОО включают в себя:

1) предположение-1:

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

2) предположение-2:

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

3) предположение-3:

совместимость ОО с контролируемыми ресурсами ОЦИ;

4) предположение-4:

корректная совместная работа САВЗ с САВЗ других производителей в случае их совместного использования в цифровой системе;

5) предположение-5:

физическая защита элементов ОЦИ, 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 функционирование ОО, руководствуясь эксплуатационной документацией.

Параграф 2. Угрозы

10. Угрозы, которым противостоит ОО:

1) угроза-1:

описание угрозы - внедрение КВ в автоматизированные рабочие места ОЦИ 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 ОЦИ при осуществлении информационного обмена;

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

вид цифровых ресурсов, потенциально подверженных угрозе - цифровые ресурсы ОЦИ, в которой установлен ОО;

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

возможные последствия реализации угрозы - проникновение компьютерных вирусов в программно-технические средства вычислительной сети ОЦИ, утечка конфиденциальной информации, нарушение режимов функционирования ОЦИ;

2) угроза-2:

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

источник угрозы - внутренний нарушитель;

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

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

вид цифровых ресурсов, потенциально подверженных угрозе - цифровые ресурсы ОЦИ, в которой установлен ОО;

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

возможные последствия реализации угрозы - проникновение компьютерных вирусов в программно-технические средства вычислительной сети ОЦИ, утечка конфиденциальной информации, нарушение режимов функционирования ОЦИ.

11. 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 ОЦИ, уязвимости технических, программных и программно-технических средств ОЦИ, которые взаимодействуют с САВЗ и могут влиять на функционирование САВЗ, недостатки механизмов управления доступом, защиты сеансов, физической защиты оборудования в ОЦИ;

вид цифровых ресурсов, потенциально подверженных угрозе - данные ФБО;

нарушаемые свойства безопасности цифровых 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 ОЦИ, уязвимости технических, программных и программно-технических средств ОЦИ, которые взаимодействуют с САВЗ и могут влиять на функционирование САВЗ, недостатки механизмов управления доступом, защиты сеансов, физической защиты оборудования в ОЦИ;

вид цифровых ресурсов, потенциально подверженные угрозе – настройки программного обеспечения САВЗ;

нарушаемые характеристики безопасности цифровых ресурсов – целостность;

возможные последствия реализации угрозы - нарушение режимов функционирования САВЗ, не обнаружение внедрения в ОЦИ 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 ОЦИ, а также специализированных инструментальных средств;

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

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

нарушаемые свойства безопасности цифровых ресурсов -целостность, доступность;

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

Параграф 3. Политика безопасности организации

12. САВЗ работает по политики безопасности организации:

1) политика безопасности-1:

механизмы регистрации предоставляют уполномоченным субъектам ОЦИ 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 ОЦИ;

3) политика безопасности-3:

управление со стороны уполномоченных субъектов ОЦИ 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 КВ объектов в заданных областях памяти и файлах;

6) политика безопасности-6:

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

7) политика безопасности-7:

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

8) политика безопасности-:

САВЗ обеспечивает возможность установки режимов выполнения обновлений БД ПКВ САВЗ.

Глава 4. Цели безопасности

Параграф 1. Цели безопасности для объекта оценки

13. 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 ОЦИ 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 ОЦИ;

3) Цель безопасности-3. Управление работой САВЗ.

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

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

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

5) цель безопасности-5. Выполнение проверок объектов.

САВЗ обеспечивают выполнение проверок с целью обнаружения КВ объектов;

6) цель безопасности-6. Режимы выполнения проверок.

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

7) цель безопасности-7. Обработка объектов.

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

14. Описание целей безопасности для среды функционирования ОО:

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

Обеспечение доступа САВЗ к данным ОЦИ, 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 ОЦИ;

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

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

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 ОЦИ (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 ОЦИ.

Глава 5. Обоснование

Параграф 1. Обоснование целей безопасности объекта оценки

15. Цели безопасности:

1) цель безопасности-1.

Достижение цели безопасности необходимо в связи с противостоянием угрозам Угроза-1, Угроза-2 и реализацией политики безопасности организации Политика безопасности-1, требуется для обеспечения надлежащей регистрации и предупреждения о любых событиях, относящихся к возможным нарушениям безопасности, возможность выборочного ознакомления с информацией о произошедших событиях;

2) цель безопасности-2.

Достижение 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 ОЦИ;

3) цель безопасности-3.

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

4) цель безопасности-4.

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

5) цель безопасности-5.

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

6) цель безопасности-6.

Достижение цели безопасности необходимо в связи с реализацией политики безопасности организации Политики безопасности-6 и обеспечивает возможность установки режимов выполнения проверок с целью обнаружения КВ объектов;

7) цель безопасности-7.

Достижение цели безопасности необходимо в связи с реализацией политики безопасности организации Политики безопасности-7 и обеспечивает возможность удаления (если удаление технически возможно) кода КВ;

8) цель безопасности-8.

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

16. 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

17. Отображение целей безопасности для среды на предположения безопасности, политики 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 ОЦИ, 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 цифровыми ресурсами ОЦИ;

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 цифровой 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 ОЦИ, 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 ОЦИ (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 ОЦИ.

Раздел 2. Профиль защиты систем обнаружения вторжений уровня сети

Глава 1. Общие положения

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

2. 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 цифровой системе.

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

4. Датчики (сенсоры) собирают информацию о пакетах данных, передаваемых в пределах ОЦИ, в которой (котором) установлены эти датчики. Датчики СОВ уровня сети реализованы в виде программного обеспечения (ПО), устанавливаемого на стандартные программно-технические платформы, а также в виде программно-технических устройств, подключаемых к ОЦИ. Анализаторы выполняют

анализ собранной датчиками информации, генерируют отчеты по результатам анализа и управляют процессами реагирования на выявленные вторжения.

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

6. 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 цифровой системе;

8) реагирование СОВ.

7. 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.

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

9. 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.

10. 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.

11. 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 ОЦИ 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) предоставление возможности чтения информации из записей аудита;

17) ограничение доступа к чтению записей аудита;

18) поиск, сортировка, упорядочение данных аудита.

12. Архитектура СОВ включает следующие компоненты:

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

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, на основании которой принимается решение о наличии вторжения;

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

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

14. Датчики уровня сети устанавливаются в разрыв канала связи контролируемого сегмента ИС путем подключения к портам сетевого оборудования ОЦИ, интегрированными в межсетевые экраны или в коммуникационное оборудование ОЦИ.

15. Анализатор обладает функциональными возможностями:

1) принимать данные от датчиков;

2) обрабатывать данные с целью выявления вторжений;

3) реагировать на выявленные вторжения.

16. Реагирование включает создание отчетов, отображение сообщения на консоли управления.

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

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

19. 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 ОЦИ СОВ уровня сети представлена в приложении 4 к настоящему ПЗ.

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

Глава 2. Среда безопасности объекта оценки

Параграф 1. Предположения безопасности

21. Предположения относительно предопределенного использования СОВ включают в себя:

1) предположение-1:

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

2) предположение-2:

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

3) предположение-3:

совместимость СОВ с элементами ОЦИ, контроль которой он осуществляет;

4) предположение-4:

физическая защита элементов ОЦИ, 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, обеспечивает надлежащее функционирование СОВ, руководствуясь эксплуатационной документацией.

Параграф 2. Угрозы

22. 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 ОЦИ с использованием штатных средств, предоставляемых ОЦИ, а также специализированных инструментальных средств;

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

вид цифровых ресурсов, потенциально подверженных угрозе - данные пользователей, конфигурационные данные, другие ресурсы ОЦИ;

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

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

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 цифровой системе;

источник угрозы - внутренние нарушители;

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

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

вид цифровых ресурсов, потенциально подверженных угрозе - данные пользователей, конфигурационные данные, другие ресурсы ОЦИ;

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

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

23. 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 ОЦИ, недостатки механизмов защиты журналов аудита СОВ;

вид цифровых ресурсов, потенциально подверженных угрозе - данные СОВ;

нарушаемые свойства безопасности цифровых 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 ОЦИ, уязвимости СОВ, внесенные на этапах проектирования и разработки, недостатки контроля программной среды ОЦИ;

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

нарушаемые свойства безопасности цифровых ресурсов - целостность, доступность;

возможные последствия реализации угрозы - нарушение режимов функционирования СОВ, не обнаружение реализуемых по отношению к ОЦИ 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 ОЦИ, уязвимости технических, программных и программно-технических средств ОЦИ, которые взаимодействуют с СОВ и могут влиять на функционирование СОВ, недостатки механизмов управления доступом, защиты сеансов, физической защиты оборудования в ОЦИ;

вид цифровых 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 ОЦИ 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 ОЦИ, а также специализированных инструментальных средств;

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

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

нарушаемые свойства безопасности цифровых ресурсов -целостность, доступность;

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

Параграф 3. Политика безопасности организации

24. СОВ следует следующим правилам политики безопасности организации:

1) политика безопасности-1:

управление параметрами СОВ, которые влияют на выполнение функций безопасности СОВ, осуществляется 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 ОЦИ 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

25. 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 ОЦИ.

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 ОЦИ 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

26. Описание целей безопасности для среды функционирования СОВ:

1) цель для среды функционирования ОО-1: доступ к данным ОЦИ.

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

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 ОЦИ, контроль которой он осуществляет;

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

Физическая защита элементов ОЦИ, 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 ОЦИ предоставляться только уполномоченным администраторам СОВ и ОЦИ;

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

27. Отображение целей безопасности для ОО на угрозы и политику безопасности организации осуществляется согласно приложению 5 к настоящему ПЗ:

1) цель безопасности-1.

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

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

3) цель безопасности-3.

Достижение 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 ОЦИ заданными методами с целью вынесения решения об обнаружении вторжения;

4) цель безопасности-4.

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

10) цель безопасности-10.

Достижение 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

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

1) цель для среды функционирования ОО-1.

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

2) цель для среды функционирования ОО-2.

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

4) цель для среды функционирования ОО-4.

Достижение 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 ОЦИ, на которых установлены компоненты СОВ, критически важные с точки зрения осуществления политики безопасности СОВ;

5) цель для среды функционирования ОО-5.

Достижение 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 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 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 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 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 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.

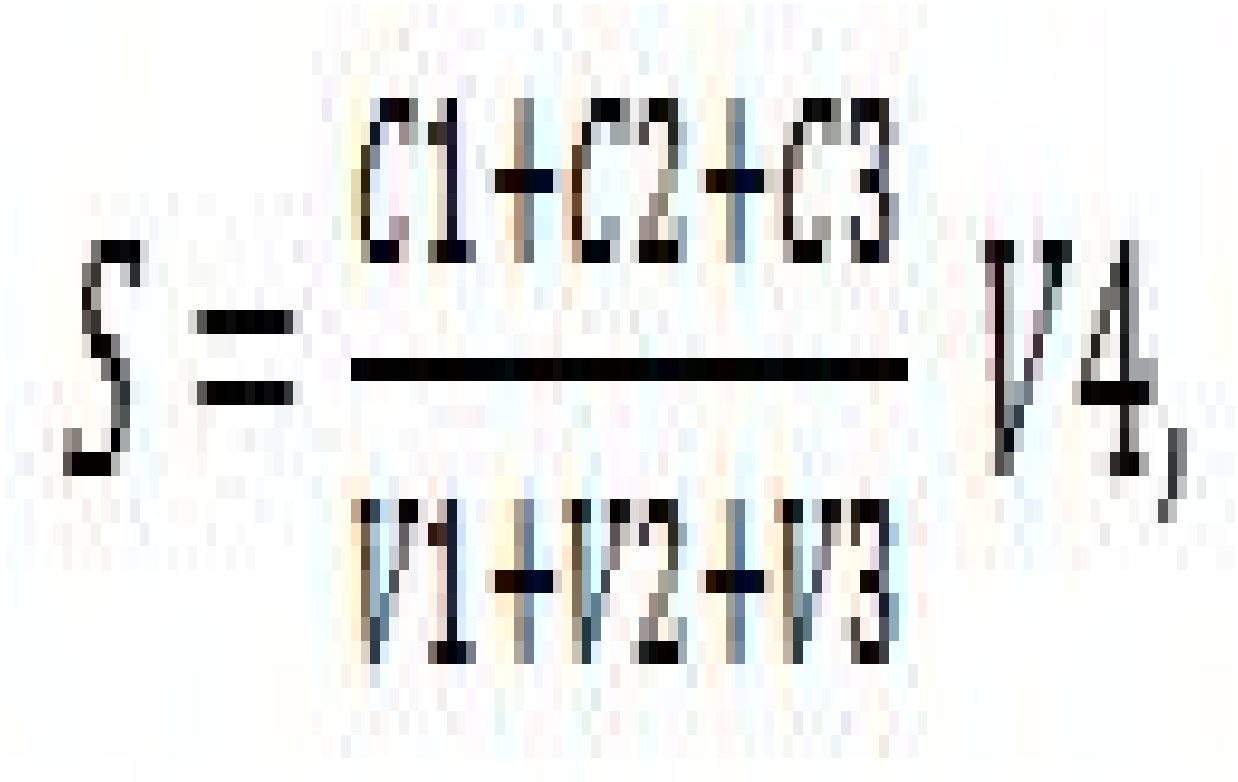
Достижение цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды Угрозы для среды-2, 3, так как обеспечивается предоставления возможности управления атрибутами безопасности компонентов СОВ и контролируемых ОЦИ только уполномоченным администраторам СОВ и ОЦИ;

12) цель для среды функционирования ОО-12.

Достижение 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

Типовая схема объекта цифровой инфраструктуры, в которой применяется средство антивирусной защиты



Приложение 2
к профилям защиты

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 безопасности-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

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 для среды функционирования ОО-6	Цель для среды функционирования ОО-7	Цель для среды функционирования ОО-8	Цель для среды функционирования ОО-9
Предположение-1	X								
Предположение-2		X							
Предположение-3			X						
Предположение-4				X					
Предположение-5					X				
Предположение-6						X			
Предположение-7							X		
Угроза среды-1					X				X
Угроза среды-2								X	X
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

Типовая схема применения в объектах цифровой инфраструктуры система обнаружения вторжений уровня сети

Приложение 5
к профилям защиты

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 безопасности-8	Цель безопасности-9	Цель безопасности-10
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									X	
Политика безопасности-10										X

Приложение 6
к профилям защиты

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 для среды функционирования ОО-6	Цель для среды функционирования ОО-7	Цель для среды функционирования ОО-8
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

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 среды функционирования ОО-6	Цель для среды функционирования ОО-7	Цель для среды функционирования ОО-8	Цель для среды функционирования ОО-9	Цель для среды функционирования ОО-10	Цель для среды функционирования ОО-11	Цель для среды функционирования ОО-12
Угроза среды-1						X		X				
Угроза среды-2					X	X		X				
Угроза среды-3				X		X		X				
Угроза среды-4							X					

Приложение 2 к приказу
Заместитель Премьер-Министра
– Министр искусственного
интеллекта и цифрового
развития
Республики Казахстан
от 3 июля 2026 года
№ 380/НҚ

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 20) статьи 7-1 Закона Республики Казахстан "О кибербезопасности".

2. Методика предназначена для разработки профилей защиты объектов цифровой инфраструктуры.

3. В настоящей Методике используются термины и определения:

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

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

3) угроза кибербезопасности (далее – угроза) – совокупность условий и факторов, создающих предпосылки к возникновению инцидента кибербезопасности;

4) профиль защиты – перечень минимальных требований к безопасности программных и технических средств, являющихся компонентами цифровых объектов;

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

6) объекты цифровой инфраструктуры (далее – ОЦИ) – совокупность материальных , технических и технологических средств, обеспечивающих размещение и среду функционирования цифровых объектов;

7) цифровая инфраструктура – совокупность объектов цифровой инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования цифровых ресурсов и предоставления доступа к ним;

Глава 2. Методика разработки профилей защиты

4. Разработка профиля защиты осуществляется с применением следующих методов:

1) метод анализа компонентов Цифрового объекта (далее – ЦО);

2) метод моделирования угроз;

3) метод анализа среды эксплуатации компонентов ЦО;

4) метод определения целей безопасности;

5) метод выбора функциональных требований безопасности;

6) метод верификации и логического обоснования профиля защиты.

5. Разработка профиля защиты включает следующие этапы:

1) идентификация компонента ЦО, для которого разрабатывается профиль защиты;

2) определение назначения компонента ЦО, его функций, условий эксплуатации и предполагаемой категории пользователей;

3) анализ архитектуры, интерфейсов взаимодействия и обрабатываемой информации компонента ЦО;

4) определение среды безопасности компонента ЦО, включая:

предположения безопасности;

потенциальные угрозы;

положения политики безопасности организации;

5) моделирование угроз, включающее:

выявление источников угроз;

определение уязвимостей;

оценку возможных последствий реализации угроз;

определение актуальных угроз;

6) формирование целей безопасности для компонента ЦО и среды его эксплуатации на основании результатов анализа угроз и политики безопасности организации;

7) определение функциональных требований безопасности, обеспечивающих реализацию целей безопасности компонента ЦО;

8) проверка согласованности требований безопасности, целей безопасности и выявленных угроз;

9) подготовка обоснования достаточности выбранных требований безопасности для обеспечения безопасности компонента ЦО;

10) оформление профиля защиты в соответствии с установленной структурой.

6. Результаты разработки профиля защиты обеспечивают:

1) идентификацию актуальных угроз компонентов ЦО;

2) определение необходимых мер защиты информации;

3) формирование функциональных требований безопасности;

4) обоснование выбранных мер защиты для обеспечения безопасности компонентов ЦО.