УДК 004 **Информационные технологии**

Юрченко Кирилл Иванович, *студент,*
ФГБОУ ВО Донской государственный технический университет

СИСТЕМЫ ПРЕДУПРЕЖДЕНИЯ КИБЕРУГРОЗ

Аннотация: С постоянно растущей зависимостью от цифровых технологий ландшафт угроз для кибератак становится все более сложным и изощренным. Киберпреступники постоянно разрабатывают новые способы взлома сетей, кражи конфиденциальных данных и нарушения работы критически важных систем. Чтобы противостоять этим угрозам, организациям необходимы продвинутые механизмы защиты, способные подавать сигналы раннего предупреждения о потенциальных вторжениях. Системы обнаружения и предотвращения вторжений (IDPS) служат важнейшими системами раннего предупреждения, активно отслеживая сетевой трафик и обнаруживая подозрительные действия. В статье исследуется значение IDPS, их функциональность, преимущества и их роль в качестве систем раннего предупреждения для защиты от киберугроз.

Ключевые слова: системы предупреждения киберугроз, киберугроза, информационная безопасность, системы обнаружения.

Annotation: With ever-increasing reliance on digital technology, the threat landscape for cyberattacks is becoming more complex and sophisticated. Cybercriminals are constantly developing new ways to hack networks, steal sensitive data, and disrupt critical systems. To counter these threats, organizations need advanced security mechanisms that can provide early warning of potential intrusions. Intrusion Detection and Prevention Systems (IDPS) serve as critical early warning systems by actively monitoring network traffic and detecting suspicious activity. This essay explores the meaning of IDPS, their functionality, benefits, and their role as early

warning systems to protect against cyber threats.

Keywords: Early warning systems for cyber threats, cyber threat, information security, detection systems.

Понимание систем обнаружения и предотвращения вторжений

Системы обнаружения и предотвращения вторжений (IDPS) — это механизмы безопасности, предназначенные для мониторинга и анализа сетевого трафика в режиме реального времени. Их основная цель - выявлять потенциальные нарушения безопасности, попытки несанкционированного доступа и вредоносные действия и реагировать на них. ВПЛ можно разделить на два основных типа:

1. Системы обнаружения вторжений (IDS): IDS пассивно отслеживают сетевой трафик, анализируя пакеты данных для обнаружения шаблонов или сигнатур, связанных с известными киберугрозами. Когда IDS идентифицирует подозрительные действия, он генерирует предупреждения для дальнейшего расследования и реагирования [1].

2. Системы предотвращения вторжений (IPS): IPS, с другой стороны, активно вмешиваются в сетевой трафик, чтобы блокировать или смягчать потенциальные угрозы. Они не только обнаруживают вредоносные действия, но и принимают немедленные меры для предотвращения вторжения.

Функциональность систем обнаружения и предотвращения вторжений

1. Мониторинг трафика: IDPS непрерывно отслеживают входящий и исходящий сетевой трафик, анализируя пакеты данных на предмет шаблонов, которые соответствуют известным сигнатурам атак или аномалиям, отклоняющимся от нормального поведения трафика.

2. Обнаружение на основе сигнатур: IDPS используют базы данных сигнатур для сравнения сетевого трафика с известными схемами атак. Когда совпадение найдено, система генерирует предупреждение и инициирует соответствующий ответ [2].

3. Обнаружение на основе аномалий: Обнаружение аномалий включает в

себя изучение нормальных моделей поведения сети с течением времени. Когда IDPS обнаруживает отклонения от установленного базового уровня, он запускает оповещение для дальнейшего расследования.

4. Реагирование и предотвращение: IP-адреса принимают упреждающие меры для предотвращения потенциальных вторжений. При обнаружении вредоносной активности IP-адреса могут блокировать вредоносный трафик, помещать затронутые системы в карантин или прерывать подозрительные подключения [3].

Преимущества систем обнаружения и предотвращения вторжений

1. Раннее обнаружение угроз: IDPS предоставляют сигналы раннего предупреждения о потенциальных киберугрозах, позволяя организациям оперативно реагировать и снижать риски до того, как они перерастут в серьезные инциденты безопасности.

2. Мониторинг в режиме реального времени: Возможности IDPS по мониторингу в режиме реального времени позволяют быстро обнаруживать вторжения и реагировать на них, сокращая время, необходимое киберпреступникам для использования уязвимостей.

3. Уменьшение ущерба: благодаря быстрому выявлению вторжений и реагированию на них ВПЛ могут предотвращать или ограничивать масштабы утечек данных, сводя к минимуму ущерб и потенциальные финансовые потери.

4. Улучшенное реагирование на инциденты: Оповещения IDPS служат ценной информацией для групп реагирования на инциденты, помогая им расследовать инциденты безопасности, понимать схемы атак и формулировать эффективные контрмеры.

5. Соответствие требованиям и нормативные акты: Многие отраслевые нормативные акты предписывают использование мер по обнаружению вторжений и предотвращению их возникновения для защиты конфиденциальных данных. IDPS помогает организациям соответствовать этим требованиям и обеспечивает соблюдение стандартов защиты данных.

Роль ВПЛ как систем раннего предупреждения

1. Проактивная защита: ВПЛ действуют как механизмы проактивной защиты, постоянно отслеживая сетевую активность для выявления потенциальных угроз и оповещения служб безопасности до того, как вторжения нанесут значительный ущерб.

2. Быстрое реагирование на инциденты: Благодаря мониторингу в режиме реального времени и раннему обнаружению IDPS способствуют быстрому реагированию на инциденты, позволяя командам безопасности оперативно сдерживать и смягчать угрозы.

3. Защита от атак нулевого дня: Обнаружение аномалий в IDPS позволяет идентифицировать неизвестные угрозы и атаки нулевого дня, которые могут не иметь предопределенной сигнатуры, повышая безопасность от возникающих угроз.

4. Улучшенная видимость сети: IDPS обеспечивают организациям большую видимость их сетевого трафика, помогая выявлять закономерности попыток несанкционированного доступа или необычного поведения, которые могут свидетельствовать о потенциальных вторжениях.

5. Сочетание с другими мерами безопасности: IDPS дополняют другие меры безопасности, такие как брандмауэры и антивирусное программное обеспечение, создавая комплексную стратегию защиты от киберугроз.

Вывод

Системы обнаружения и предотвращения вторжений (IDPS) действуют как системы раннего предупреждения, активно отслеживая сетевой трафик и предоставляя оповещения в режиме реального времени о потенциальных киберугрозах. Их способность обнаруживать вредоносные действия и быстро реагировать на них имеет решающее значение для защиты конфиденциальных данных и критически важных систем. Используя IDPS как часть комплексной стратегии кибербезопасности, организации могут повысить свою способность защищаться от широкого спектра кибератак, включая известные и неизвестные угрозы. Поскольку киберугрозы продолжают развиваться, ВПЛ будут оставаться жизненно важными инструментами поддержания целостности и безопасности

цифровых активов во все более взаимосвязанном мире.

Библиографический список:

1. Басыня Е. А. Самоорганизующаяся система управления трафиком вычислительной сети / Е. А. Басыня, Г. А. Французова, А. В. Гунько // Доклады Томского государственного университета систем управления и радиоэлектроники. - 2014. - № 1 (31). - С. 179-184.

2. Сафронов А. В. Применение метода согласования балансов для повышения эффективности информационно - измерительной системы при опредлении ТЭП ТЭЦ / А. В. Сафронов // Сборник трудов ХУ11 Международной научно-практической конференции студентов, аспирантов и молодых ученых. 9-13 апреля 2012, Томск: Изд-воТПУ, 2012. - С.237 - 238.

3. Basinya E. A. Methods of self-organization in providing network security / E. A. Basinya, G. A. Frantsuzova, A. У. Gunko // Global Science and Innovation: materials of the 1 intern. sci. conf., USA, Chicago, 17-18 Dec. 2013. - Chicago: Accent Graphics communications 2013. - Vol. 2. - P. 386-389.