Представленный способ уточнения данных инклинометрии скважин был протестирован на нескольких траекториях, полученных прибором ИГН73-100/80, и показал возможность коррекции координат точки входа в круг допуска на 5-30 метров при различных уровнях шума.

Литература

Cortes, C., Vapnik, V., 1995. Support-vector networks. Machine learning 20, 273–297.

Smola, A.J., Schölkopf, B., 2004. A tutorial on support vector regression. Statistics and computing 14, 199–222.

Yeh, C.Y., Huang, C.W., Lee, S.J., 2011. A multiple-kernel support vector regression approach for stock market price forecasting. Expert Systems with Applications 38, 2177–2186.

М.А. Борисов, А.А. Гуськов, С.И. Кошелев, 2016. Повышение точности определения траектории скважины гироинклинометром за счет вторичной обработки данных. Приволжский научный вестник № 12-2 (64) – 2016, 11-14.

ВЕРОЯТНОСТНЫЙ ПОДХОД К ОЦЕНКЕ ЗАЩИЩЁННОСТИ ИНФОРМАЦИИ ОТ УГРОЗ

Титов Михаил Юрьевич
кандидат тех. наук, с.н.с
РТУ МИРЭА
г. Москва
Карасев Павел Игоревич
кандидат тех. наук, доцент
РТУ МИРЭА
г. Москва
Пушкин Павел Юрьевич
кандидат тех. наук, доцент
РТУ МИРЭА
г. Москва
Титова Маргарита Михайловна
инженер-конструктор первой категории
ООО «Прогресстех»
г. Москва

PROBABLE APPROACH TO SAFETY ASSESSMENT INFORMATION FROM THREATS

Titov Michail
Candidate of Science, assistant professor
of RTU MIREA, Moscow
Karasev Pavel
Candidate of Science, assistant professor
of RTU MIREA, Moscow
Pushkin Pavel
Candidate of Science, assistant professor
of RTU MIREA, Moscow
Titova Margarita
design engineer of the first category
LLC "Progresstech"
DOI: 10.31618/NAS.2413-5291.2021.1.74.515

АННОТАЦИЯ

Общеизвестно, что основная цель защиты информации – обеспечение заданного уровня её безопасности. Заданный уровень безопасности информации характеризуется состоянием её защищённости от угроз, при котором обеспечивается допустимый риск её уничтожения, изменения, хищения, а также блокирования.

Риски зависят от уровня инженерно-технической защиты информации (ИТЗИ), который определяется ресурсами системы. Чем больше ресурс на защиту информации, тем выше уровень безопасности. При неограниченном ресурсе можно получить сколь угодно малую вероятность реализации угрозы.

ABSTRACT

It is well known that the main goal of information protection is to ensure a given level of its security. The specified level of information security is characterized by the state of its protection from threats, which provides an acceptable risk of its destruction, alteration, theft, and blocking.

Risks depend on the level of engineering and technical protection of information

(ITZI), which is determined by the resources of the system. The more resource for information protection, the higher the level of security. With an unlimited resource, you can get an arbitrarily small probability of a threat being realized.

Ключевые слова: оценка угроз информационный безопасности, качество, вероятностный подход.
Keywords: information security threat assessment, quality, probabilistic approach.

Реализация угроз осуществляется с различной вероятностью, характеризующей степень риска. Ущерб может проявляться в различных формах (неполучение прибыли; дополнительные затраты на замену перспективных технологий, ставших достоянием конкурента и т.д.).

Ущерб от реализации угрозы можно представить в виде следующего соотношения:

$$C_{\text{у}} = C_{\text{и}} = P_{\text{у}}, \qquad (1)$$

где: $C_{\text{у}}$ - ущерб от реализации угрозы, ден. ед.;

$C_{\text{и}}$ – цена информации, ден. ед.;

$P_{\text{у}}$ – вероятность реализации угрозы.

Величину ущерба можно рассматривать как возможные косвенные расходы, а ресурс – как прямые $C_{\text{пр}}$. Следовательно, общие расходы на информацию составят:

$$C_{\text{ри}} = C_{\text{пр}} + C_{\text{кр}}, \qquad (2)$$

где: $C_{\text{ри}}$ - общие расходы на информацию, ден. ед.;

$C_{\text{пр}}$ – прямые расходы на информацию, ден. ед.;

$C_{\text{кр}}$ – косвенные расходы на информацию, ден. ед.

Необходимо учитывать, что косвенные расходы обратно пропорциональны прямым расходам. В результате зависимость суммарных расходов на информацию от прямых качественно можно представить в виде следующих графиков (Рис. 1).

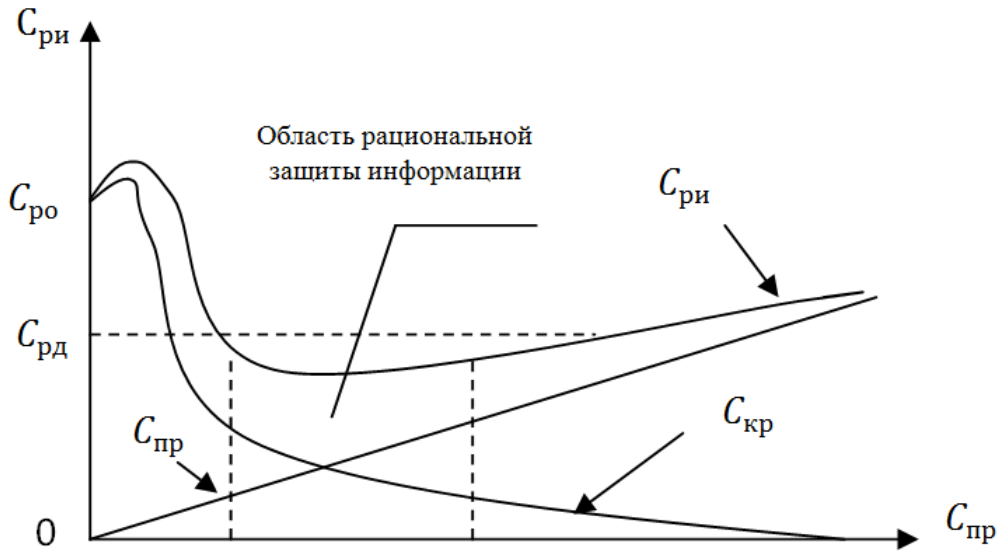

Рисунок 1. Графики зависимости суммарных расходов от прямых

Рост суммарных расходов на информацию при малых прямых расходах вызван тем, что эффект защиты проявляется тогда, когда прямые расходы превышают некоторую критическую величину. Из графиков следует, что при некоторых прямых расходах наблюдается область с минимальными суммарными расходами на информацию – область рациональной защиты информации.

Знание конкретных угроз позволяет определить рациональные меры защиты информации от этих угроз или минимизировать вероятность их реализации.

Выбор любой меры защиты информации производится по показателям оценки эффективности (ПОЭ), которые учитывают степень выполнения задачи и затраты ресурса на её решение. Многообразие угроз безопасности информации порождает многообразие мер её защиты. Эффективность каждой меры защиты безопасности информации оценивается частными показателями эффективности (ЧПЭ), которые подразделяются на функциональные и экономические.

Функциональные показатели характеризуют уровень безопасности информации, а экономические – расходы на её обеспечение. Поскольку уровень безопасности информации определяется величиной потенциального ущерба от реализации угроз, то в качестве частных функциональных показателей эффективности защиты информации используются показатели количества и качества информации, попавшей к злоумышленнику, а также характеристики реально возникающих угроз безопасности информации.

Эффективность системы защиты информации в целом определяется глобальными функциональным и экономическим показателями. В качестве функционального глобального показателя используется в основном «взвешенная» сумма частных функциональных показателей. Глобальный экономический показатель представляет собой меру суммарных расходов на информацию.

Пусть ω_i – значение *i*-го частного показателя, то глобальный показатель определится как:

$$W_{\text{г}} = \sum \mu_i \omega_i \text{ , причём } \sum \mu_i = 1,$$

где: i – целое положительное число.

Коэффициент μ_i характеризует вес частного показателя.

Эффективность тем выше, чем ниже расходы при одинаковом уровне безопасности информации или чем больше уровень её безопасности при одинаковых расходах. Первый подход к оценке эффективности используется при отсутствии жёстких ограничений на ресурс, выделяемый для защиты информации, второй – при заданном ресурсе.

Технология анализа защищённости высоконадежных систем

В любых ВС, использующих КИС, приходится регулярно проверять, насколько реализованные или используемые механизмы защиты информации соответствуют положениям принятой в организации политики безопасности. Такая задача периодически возникает при изменении и обновлении компонентов КИС, изменении конфигурации ОС и т.п.

Администраторы сетей ограничены по времени на проведение такого рода проверок для всех узлов корпоративной сети. Поэтому специалисты отделов защиты информации нуждаются в средствах, облегчающих анализ защищённости используемых механизмов обеспечения информационной безопасности.

Использование средств анализа защищённости (САЗ) позволяет определить уязвимости на узлах корпоративной сети и устранить их до того, как ими воспользуются злоумышленники.

САЗ работают на первом этапе осуществления атаки. Обнаруживая и своевременно устраняя уязвимости, они предотвращают саму возможность реализации атаки, что позволяет снизить затраты на эксплуатацию средств защиты.

САЗ могут функционировать на сетевом уровне, уровне ОС и уровне приложения. Они могут проводить поиск уязвимостей, постепенно наращивая число проверок в КИС, исследуя все её уровни.

ВЫВОД

Наибольшее распространение получили САЗ сетевых сервисов и протоколов. Это обусловлено универсальностью используемых протоколов.

С одной стороны, изученность и повсеместное использование таких протоколов, как IP, TCP, HTTP, FTP, SMTP позволяют с высокой степенью эффективности осуществлять обмен информацией в подсистемах ВС. С другой стороны, эти протоколы не обеспечивают безопасную передачу данных. Поэтому должную защиту КИС СИО ВССДН в сетевом окружении могут обеспечивать только протоколы защищенности такие, как: SSL (SSL3), SSH, IPSec, TLS (TLS2).

Вторыми по распространению являются САЗ ОС. Это также обусловлено универсальностью и распространённостью некоторых ОС (например, UNIX и Windows NT). САЗ приложений пока существуют только для широко распространённых прикладных систем типа Web-браузеры и СУБД.

Применение САЗ позволяет быстро определить все узлы корпоративной сети, доступные в момент проведения тестирования, выявить все используемые в сети сервисы и протоколы, их настройки и возможности для несанкционированного воздействия (как изнутри корпоративной сети, так и снаружи). По результатам сканирования эти средства вырабатывают рекомендации и пошаговые меры, позволяющие устранить выявленные недостатки.

Литература:

1. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. - 384 с.

2. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.

3. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с.

4. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. — 416 с.

5. Антонюк Л.Я., Семисошенко М.А. Адаптивная радиосвязь в системах связи специального назначения // Электросвязь, 2007, №5, С. 17-20.