© Al-Dalvash A. Models of optimal fuel functioning of remote access security in information networks // Ukrainian Scientific Journal of Information Security, 2021, vol. 26, issue 3, pp. 126-131..

DOI: 10.18372/2225-5036.27.16513

МОДЕЛИ ОПТИМАЛЬНОГО ФУНКЦИОНИРОВАНИЯ БЕЗОПАСНОСТИ УДАЛЕННОГО ДОСТУПА В ИНФОРМАЦИОННЫХ СЕТЯХ

Аль-Далваш Абдуллах

АЛЬ-ДАЛВАШ Аблуллах Фоуад
Год и место рождения: 1991 год, г. Самарра, Ірак.
Образование: Донецкий национальній университет имени Василия Стуса, 2018 г.
Должность: аспирант, Национальній авыационный университет.
Научные интересы: информационная безопасность, кибербезопасность в информационных сетях.
Публикации: 10 научных публикации, среди которых научные статьи и тезисы.
E-mail: abdullah.dalosh@gmail.com.
ORCID: 0000-0001-1003-9182.

Аннотация. *В статье рассмотрен ряд модулей по безопасности в информационных сетях, что позволяет оптимально регламентировать доступ в локальную информационную сеть с внешних сетей с точки зрения безопасности информации; определены численные значения возможностей несанкционированного доступа для данного вида соединения, выбранного на основе полученных данных, для оптимального выбора защитных механизмов. В статье рассмотрен ряд модулей по безопасности в информационных сетях, что позволяет оптимально регламентировать доступ в локальную информационную сеть с внешних сетей с точки зрения безопасности информации; определены численные значения возможностей несанкционированного доступа для данного вида соединения, выбранного на основе полученных данных, для оптимального выбора защитных механизмов. В статье рассмотрен ряд модулей по безопасности в информационных сетях, что позволяет оптимально регламентировать доступ в локальную информационную сеть с внешних сетей с точки зрения безопасности информации; определены численные значения возможностей несанкционированного доступа для данного вида соединения, выбранного на основе полученных данных, для оптимального выбора защитных механизмов.*

Ключевые слова: *информационные сети, удаленный доступ, оптимальное функционирование безопасности, безопасность информационных сетей, безопасность информации.*

Введение

Сегодня методы и средства несанкционированного доступа и информации в сфере с широким применением ПЭВМ, взаимодействующих через локальные и глобальные сети, приобрели такую популярность, что нередко само понятие «защита информации» применяется положительно в смысле защиты информации, обрабатываемой в автоматизированных системах (АС).

Однако, как считают специалисты, защиту информации (ЗИ) в сетях следует выделить в отдельный канал, равноценный другим техническим каналам утечки информации [1]. Конечно, в определенном смысле утечка информации по информационным сетям также возникает вследствии несовершенства программно-аппаратных решений, реализованных в АС.

Но, тем не менее, пользуясь подобными изъянами в архитектуре АС и информационных сетях (ИС), злоумышленник может использовать их ресурсы и процессы для проведения несанкционированного доступа (НСД) к информации.

Количество методов и средств НСД к информации из АС и ИС при удаленном доступе значительно шире и достаточно сильно зависит от используемой операционной системы (ОС), настройки параметров безопасности и т.п.

Как не парадоксально, но наиболее эффективными (с некоторыми оговорами) при удаленном доступе являются системы и сети, работающие под управлением операционных систем, которые наиболее всего уязвимы при локальном доступе. Это связано с тем, что в них практически отсутствуют развитые средства, предоставляемые собой внешние по отношению к ядру таких систем модули, слабо интегрированные с остальными компонентами подобных простейших ОС. Поэтому, если использовать АС, работающую под управлением такой ОС, то выполняя простейшие правила безопасности (например, не предоставление доступа по сети к файлам и папкам своего компьютера), позволит системе обладать более высокой степенью устойчивости к НСД [1,2,3].

Следует отметить, что за редким исключением большинство современных ОС при настройке параметров, принятых по умолчанию, являются не безопасными с точки зрения функционирования в информационных сетях [3].

Поскольку полное описание методов и средств несанкционированного получения информации из АС при удаленном доступе может занять объем, значительно превышающий объем данной статьи, поэтому основные из них, готовые использоваться большинством злоумышленников, приведены на схеме (рис. 1) [1].

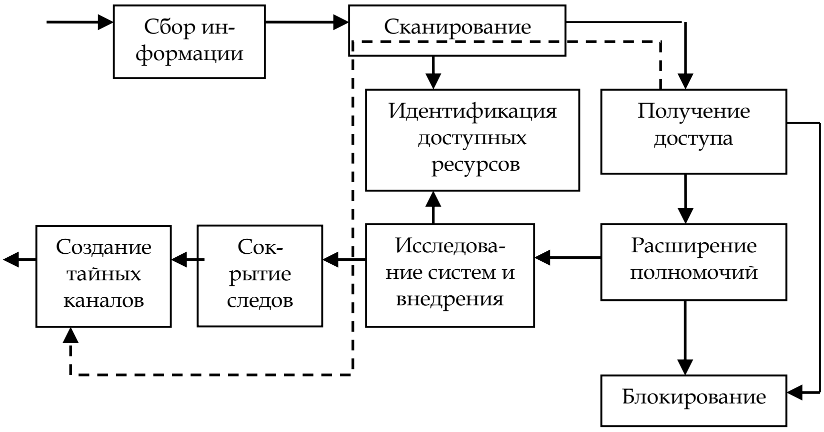

Рис. 1 Схема несанкционированного доступа к информации из АС при удалённом доступе

Основная часть

При построении модели безопасного доступа к информации упор делается на сопоставление имеющихся запрещенных средств (активных и регулярно использованных) и степени жесткости политики безопасности в АС и ИС в отношении контроля удаленного доступа (в общем случае контроль доступа подразумевает сохранение целостности информации, доступности и недопущения факта ознакомления с ней в процессе передачи, обработки и хранения в самой информационной сети) и соблюдение конфиденциальности информации при её передаче по информационным сетям.

При этом учитывается статистика случаев НСД в ИС, имеющих место ранее. Ниже приведена таблица показателей, которыми оперирует модель отдаленного доступа.

Модель безопасного модемного соединения

Расчетную вероятность несанкционированного доступа в локальную информационную сеть через модемное соединение можно определить следующим образом:

$$P_{IA}^{MI} = M_{QNT} \cdot M_{IMC} \cdot D \cdot$$
$$\cdot P(1 - M_{ID_1 AUTEN} \cdot M_{USG})(1 - M_{FILTR})\,,$$

где P – вероятность совершения попытки НСД в информационные сети через контролируемое соединение.

Определяется методом экспертных оценок, путём учёта, статистики, проявления внешних угроз в локальных сетях;

η – количество дней в году, в течении которых сеть полностью функционирует и связана с удаленными сетями контролируемым доступом;

M_{USG} – численный эквивалент синтаксического показателя M_{USG}, принимающий значение: минимальный – 0,3; низкий – 0,5; средний – 0,8; высокий – 0,9; максимальный – 0,97;

M_{FILTR} – численный эквивалент синтаксического показателя M_{FILTR}, принимающий значение: минимальный – 0,1; низкий – 0,3; средний – 0,5; высокий – 0,8; максимальный – 0,95.

Экспериментальная вероятность НСД в локальной информационной сети через модемное соединение, определяемая за период функционирования локальной информационной сети, равна:

$$P_{IA}^{M^{11}} = M_{IA} \wedge M_{FREQ} \cdot D(100 - M_{PER}).$$

Общая вероятность НСД локальной ИС через модемное соединение определяется соответственно как

$$P_{IA}^{M} = P_{IA}^{M^{1}}(1 - K_{FUNC}) + P_{IA}^{M^{11}} K_{FUNC}\,,$$

где K_{FUNC} – численный коэффициент, учитывающий время функционирования локальной ИС, за которое велась статистическая обработка случаев НСД (определялись коэффициенты $R_{1A}, R_{FREQ}, R_{PER}$).

K_{FUNC} соответственно принимает значение: 0 – менее года; 0,2 – от года до двух лет; 0,5 – 2 $\div$ 4 года;

0,8 – 4 ÷ 7 лет; 0,9 – более семи лет.

Как видно из выражения, экспериментальная вероятность (определяемая путем учета статистической обработки случаев НСД за период функционирования локальной ИС) имеет тем больший вклад в определении общей вероятности, чем за более длительный срок собраны данные о попытках взломов и атаке, и, соответственно, наоборот, при отсутствии продолжительных наблюдений общая вероятность полностью определяется расчетной вероятностью $P_{IA}^{M^1}$.

Таблица 1

Показатели модели удаленного доступа

Наименование	Тип	Применение
Модемное соединение		
M_{QNT}	Численный	Количество модемных линий
$M_{ID_I AUTEN}$	Логический	Наличие встроенных в модем алгоритмов идентификации и аутентификации
M_{USG}	Синтаксический	Схемы использования алгоритмов идентификации и аутентификации
M_{ING}	Численный	Среднее число с входящих запросов на линии
M_{IMP}	Синтаксический	Важность ресурсов, к которым имеется удалённый доступ
M_{IA}	Логический	Случаи НСД в сеть через модем
M_{FREQ}	Численный	Число случаев НСД
M_{PER}	Численный	Процент пресечения НСД в сеть через модем
M_{FILTR}	Логический	Использование средств фильтрации и запросов
M_{SEC}	Синтаксический	Степень жесткости политики безопасности модемного соединения
Соединение через роутер		
R_{ACT}	Синтаксический	Степень активности доступа и сети через WAN
R_{TRST}	Синтаксический	Степень доверия к пользователям, имеющим доступ к сети
R_{QLFC}	Синтаксический	Степень квалификации администратора сети
R_{IA}	Логический	Случай НСД в сеть через роутер
R_{FREQ}	Численный	Частота случаев НСД
R_{PER}	Численный	Процент пресечения НСД в сеть через роутер
R_{SEC}	Синтаксический	Степень жесткости политики безопасности модемного соединения
Защита информации в информационных сетях		
C_{CHNL}	Логический	Передается ли верная информация по незащищённой информационной сети
C_{VOL}	Синтаксический	Объемы передающиеся по информационной сети
C_{IMP}	Синтаксический	Важность передающейся информации по сети
C_{CRIPT}	Синтаксический	Степень использования криптографических методов
C_{CONF}	Синтаксический	Степень жесткости политики соблюдения конфиденциальности данных
Выход в интернет		
R_{FW}	Логический	Используется ли система Firewall
R_{FWUSG}	Синтаксический	Степень использования защитных средств
R_{SECMAN}	Логический	Наличие лица ответственного за безопасность
K_{AVIR}	Синтаксический	Степень использования антивирусных методов
K_{JAV}	Логический	Запрещен ли прогон Java-апплетов (левых интерактивных программ)

K_{CERT}	Логический	Загружаются ли страницы только с сертифицированных WEB-сайтов
K_{IMPRT}	Синтаксический	Степень использования за импортом программ
K_{TRN}	Синтаксический	Степень обучения пользователя безопасности

Затем расчетная вероятность НСД в локальной ИС P_{IA}^{M} сопоставляется с синтаксическим показателем $M_{IMP},_{SEC}$ определяемого соотношения M_{IMP} и M_{SEC} (табл.2).

Рассчитанная вероятность для недавно запущенной ИС должна всегда быть ниже приведенной в табл.2 для соответствующей величины показателей $M_{IMP},_{SEC}$. На основе разницы рассчитанной величины P_{IA}^{M} и приведенной в табл.2 определяется необходимый набор значущих средств.

При повторном моделировании вероятности НСД с учетом новых показателей стремятся величину P_{IA}^{M} довести до оптимальной в соответствии табл.2.

Таблица 2

Сопоставление показателей P_{IA}^{M} и $M_{IMP},_{SEC}$

$M_{IMP},_{SEC}$	P_{IA}^{M}
минимальный	>0,15
низкий	$0{,}1 \div 0{,}15$
средний	$0{,}03 \div 0{,}1$
высокий	$0{,}01 \div 0{,}03$
максимальный	<0,01

Примечание. Вероятность удачной попытки НСД приведены за период времени равный одному году.

Модуль безопасного соединения через роутер

Расчетную вероятность НСД в локальную ИС через роутер по аналогии с модемным соединением можно определить следующим образом:

$$P_{IA}^{M} = DPR_{ACT}(1-R_{TRST})(1-R_{QLFC}),$$

где P – вероятность совершения попытки НСД в локальную сеть через ограниченное соединение. Также определяется методом экспериментальных оценок путем учета статистики проявления внешних угроз в локальных ИС;

R_{ACT} – численный эквивалент синтаксического показателя R_{ACT}, принимающий значения: минимальный – 0,1; низкий – 0,25; средний – 0,5; высокий – 0,85; максимальный – 1;

R_{TRST} – численный эквивалент синтаксического показателя R_{TRST}, принимающий значения: минимальный – 0; низкий – 0,2; средний – 0,4; высокий – 0,6; максимальный – 0,75;

R_{QLFC} – численный эквивалент синтаксического показателя R_{QLFC}, принимающий значения: минимальный – 0; низкий – 0,2; средний – 0,5; высокий – 0,8; максимальный – 0,95;

Экспериментальная вероятность НСД в локальную ИС через роутер, определяемая за период функционирования сети, равна:

$$P_{IA}^{R^{11}} = R_{IA} \wedge R_{FREQ} \cdot D(100 - R_{PER}).$$

Общая вероятность НСД в локальную ИС через роутер определяется, соответственно, как:

$$P_{IA}^{R} = P_{IA}^{R^{1}}(1-K_{FUNC}) + P_{IA}^{R^{11}}K_{FUNC},$$

где K_{FUNC} – соответственно принимает значения: 0 – меньше года; 0,2 – от года до двух лет; 0,5 – $2 \div 4$ года; 0,8 – $4 \div 7$ лет; 0,9 – более семи лет. Теперь можем рассчитать вероятность НСД в локальной ИС P_{IA}^{R}, сопоставляя с синтаксическим показателем $R_{IMP},_{SEC}$, определяемого соотношением показателей R_{IMP} и R_{SEC} (приведены в табл.3).

Модуль защиты информации в информационных сетях. Эта модель предполагает вычисление вероятности нарушения конфиденциальности при передаче информации по незащищенным ИС.

$$P_{C} = C_{CHNL} \wedge PC_{VOL}(1-C_{CRIDT}),$$

где P – вероятность перехвата информации в магистральных ИС. Она определяется методом экспертных оценок путем учета статистических проявлений внешних угроз в распределенных сетях;

C_{VOL} – численный эквивалент синтаксического показателя C_{VOL}, принимающий значения: минимальный – 0,1; низкий – 0,2; средний – 0,5; высокий – 0,8; максимальный – 1;

C_{CRIPT} – численный эквивалент синтаксического показателя C_{CRIPT}, принимающий значения: минимальный – 0,5; низкий – 0,7; средний – 0,8; высокий – 0,95; максимальный – 0,999.

В этой модели не представляется возможность учитывать статистику перехвата информационных сообщений при передаче через магистральные ИС, т.к. факт перехвата или несанкционированного ознакомления с информацией в распределяемых ИС практически установить невозможно.

Основной упор в модели делается на применение криптографических средств, позволяющих свести вероятность несанкционированного ознакомления к нулю.

Сейчас рассчитывая вероятность нарушения конфиденциальности при передачи информации по незащищенным ИС P_{C} сопоставляется с синтаксическим показателем $C_{IMP},_{SEC}$, определяемого соответственно C_{IMP} и C_{SEC}, приведено в табл.4, подобно предыдущим моделям.

Таблица 3

Соотношение показателей $R_{IMP,SEC}$ и R_{IA}^{M}

$R_{IMP,SEC}$	R_{IA}^{M}
минимальный	>0,15
низкий	0,1-0,15
средний	0,03- 0,1
высокий	0,01- 0,03
максимальный	<0,01

Таблица 4

Соотношение показателей $C_{IMP,SEC}$ и P_C

$C_{IMP,SEC}$	P_C
Минимальный	>0,001
Низкий	0,001-0,0001
Средний	0,0001- 0,000001
Высокий	0,000001- 0,0000001
Максимальный	<0,0000001

Модель безопасности Internet-соединения

Сеть Internet – это многогранная и развивающаяся, живущая своей жизнью, и в то же время являющаяся неотъемлемой от нашей жизни информационная среда, в которой существуют методы и средства, позволяющие решать задачи информации в земной среде. Основное значение любой сети (в том числе и Internet) состоит в обязанности доставить необходимую информацию пользователю.

Причем, системы защиты информации в сети должны способствовать эффективному выполнению основной функции ИС Internet современному обмену информацией. Иначе говоря, не ИС делается под систему защиты, а система защиты помогает ИС (в том числе и Internet) и является вспомогательным (но очень верным) компонентом. Из этого следует, что прежде чем переходить к обеспечению безопасности сети, необходимо определиться с моделью самой ИС. [4] Прежде всего необходимо определиться с угрозами самой сети. Это возможность осуществления действия, направляемого против объекта защиты (сети), проявляемая в опасности искажений и потерь информации.

Необходимо оговорит, что речь идет не обо всей информации, а только о той ее части, которая, по мнению пользователя, имеет определенную ценность или подлежит защите согласно домена [5]. Необходимо также учитывать, что источник угроз безопасности может находиться как внутри сети, та и вовне.

Сопоставление угроз информации в ИС и группы методов их противодействия позволило решить, такими способами какие угрозы наиболее целесообразно нейтрализовать, а также определить рациональное соотношение групп методов при распределении средств, выделенных на обеспечение безопасности информации в ИС.

Можно выделить целый ряд причин, по которым нужно обеспечить информационную безопасность ИС, а также Internet:

Во-первых, разнообразные функции обеспечения информационной безопасности достаточно сильно интегрированы в существующие технологии построения ИС и систем;

Во-вторых, современные информационные технологии немыслимы без активного пользования публичных сервисов, представленных ИС и в первую очередь, Internet. По этой причине ИС необходимо назначить тем или иным способом к открытым сетям, что можно делать только при обеспечении безопасности соединения;

В-третьих, грамотно построенная и реализованная информационная безопасность может существенно расширить функциональные возможности ИС:

- Построение системы удаленного защищенного доступа пользователей к информационным ресурсам ИС.
- Использование Internet-коммуникаций для передачи информации между различными пользователями и т.д. [4,5]. Поэтому модель безопасного Internet-соединения в соответствии со степенью угроз и рисков локальной ИС подразумевает наличие набора защитных средств, суммарный весовой коэффициент, который согласно табл.5 находится в пределах: низкий риск – 0,3: средний риск - 4 ÷ 10; высокий риск – более 10.

Таблица 5

Суммарные весовые коэффициенты

K_{TRN}	K_{JAV}	K_{CERT}	K_{IMPRT}	K_{AVIR}	$R_{SEC,MAN}$	$R_{FW,USG}$
Низкий – 0 Средний – 1 Высокий - 3	Да -1 Нет - 0	Да -1 Нет - 0	Низкий – 0 Средний – 2 Высокий - 4	Низкий – 0 Средний – 3 Высокий - 5	Да -5 Нет - 0	Низкий – 1 Средний – 4 Высокий - 7

Выводы

Описание модели позволяет оптимально регламентировать доступ в локальную ИС из внешних сетей с точки зрения безопасности информации, определить численные значения вероятностей несанкционированного доступа для данного выше соединения, выбрать на основе полученных данных оптимальный набор защитных механизмов. При оценке вероятностей успешных закономерных действий принимается во внимание как перечень существующих средств защиты, так и данных о попытках несанкционированных действий за время функционирования локальной сети, что позволяет получить более точные вероятностные значения.

Модели могут применяться как на стадии проектирования сети с возможностью удаленного доступа, так и в процессе ее эксплуатации.

Литература

[1] Ленков С.В. Методы и средства защиты информации. Том 1. *Несанкционированное получение информации* / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко – К: Арий, 2008. – 464 с.

[2] Домарев В.В. *Защита информации и безопасность компьютерных систем* / В.В. Домарев – К: Изд. «Дия Софт», 1999.- 480 с.

[3] Соколов А.В. *Защита информации в распределенных нормативных сетях и системах* / А.В. Соколов, В.Ф. Шаньчин – М: ДМК Пресс, 2002 – 656 с.

[4] Vacca J. *Internet Security Secrets* – Chicago: IDG Books Worldwide, Inc., 1996. – 505 p.

[5] Федотов Е.В. механизмы возможных атак в сети Internet / Е.В. Федотов //*Защита информации. Сб. науч. Трудов НАУ* – К:НАУ, 2001. – С. 30-43.

УДК 004.681.3

Аль-Далваш А.

МОДЕЛІ ОПТИМАЛЬНОГО ФУЕКЦІОНУВАННЯ БЕЗПЕКИ ВІДДАЛЕННОГО ДОСТУПУ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ

Анотація. *У статті розглянуто ряд модулів безпеки в інформаційних мережах, що дозволяє оптимально регламентувати доступ до локальної інформаційної мережі із зовнішніх мереж з точки зору безпеки інформації; визначено чисельні значення можливостей несанкціонованого доступу даного виду з'єднання, обраного з урахуванням отриманих даних, для оптимального вибору захисних механізмів. У статті розглянуто ряд модулів безпеки в інформаційних мережах, що дозволяє оптимально регламентувати доступ до локальної інформаційної мережі із зовнішніх мереж з точки зору безпеки інформації; визначено чисельні значення можливостей несанкціонованого доступу даного виду з'єднання, обраного з урахуванням отриманих даних, для оптимального вибору захисних механізмів. У статті розглянуто ряд модулів безпеки в інформаційних мережах, що дозволяє оптимально регламентувати доступ до локальної інформаційної мережі із зовнішніх мереж з точки зору безпеки інформації; визначено чисельні значення можливостей несанкціонованого доступу даного виду з'єднання, обраного з урахуванням отриманих даних, для оптимального вибору захисних механізмів.*

Ключові слова: *інформаційні мережі, віддалений доступ, оптимальне функціонування безпеки, безпека інформаційних мереж, безпека інформації.*

Al-Dalvash A.

MODELS OF OPTIMAL FUEL FUNCTIONING OF REMOTE ACCESS SECURITY IN INFORMATION NETWORKS

Abstract. *The article considers a number of security modules in information networks, which allows to optimally regulate access to the local information network from external networks in terms of information security; the numerical values of the possibilities of unauthorized access to this type of connection, selected taking into account the obtained data, for the optimal choice of security mechanisms are determined. The article considers a number of security modules in information networks, which allows to optimally regulate access to the local information network from external networks in terms of information security; the numerical values of the possibilities of unauthorized access to this type of connection, selected taking into account the obtained data, for the optimal choice of security mechanisms are determined. The article considers a number of security modules in information networks, which allows to optimally regulate access to the local information network from external networks in terms of information security; the numerical values of the possibilities of unauthorized access to this type of connection, selected taking into account the obtained data, for the optimal choice of security mechanisms are determined.*

Keywords: *information networks, remote access, optimal security functioning, information networks security, information security.*

Аль-Далваш Аблуллах Фоуад, аспірант, Національний авіаційний університет.
Аль-Далваш Аблуллах Фоуад, аспирант, Национальный авиационный университет.
Al-Dalvash Ablullah Fowad, graduate student, National Aviation University.

Отримано *12 листопада 2021 року*, затверджено редколегією *17 грудня 2021 року*