ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ НА ОСНОВЕ КАЧЕСТВЕННЫХ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ

Алефиренко В.М.
к.т.н., доцент, Белорусский Государственный Университет Информатики и Радиоэлектроники,
Чопик К.В.
Магистрант, Белорусский Государственный Университет Информатики и Радиоэлектроники,
Шарый Д.Н.
Магистрант, Белорусский Государственный Университет Информатики и Радиоэлектроники,

THE SECURITY LEVEL ASSESSMENT OF THE ENTERPRISE LOCAL NETWORK BASED ON QUALITY INDICATORS OF SECURITY

Alefirenko V.
Associated professor, Belarus State University of Informatics and Radioelectronics, Ph. D,
Chopik K.
Master student, Belarus State University of Informatics and Radioelectronics,
Sharyi D.
Master student, Belarus State University of Informatics and Radioelectronics,

Аннотация

В статье предложен алгоритм оценки уровня защищенности локальной компьютерной сети, включающий в себя систему различных показателей защищенности и комплекс формул, используемых для их расчета.

Оценка уровня защищенности проводилась на основе качественных методов анализа рисков. Также приведен пример оценки защищенности конкретной локальной компьютерной сети. Проведено моделирование локальной вычислительной сети, которое помогло выявить зависимость уровня защищенности от количества автоматизированных рабочих мест, имеющих высокую сложность уровня доступа.

Abstract

The article offers an algorithm for evaluating the level of security of a local computer network, which includes a system of various security indicators and a set of formulas used for their calculation. The level of security was assessed based on qualitative methods of risk analysis. An example of evaluating the security of a specific local computer network is also provided. A simulation of the local computer network was performed, which helped to identify the dependence of the security level on the number of automated workplaces with a high complexity of the access level.

Ключевые слова: информационная инфраструктура, безопасность, информационные системы, компьютерные сети, модели оценки защищенности, показатели защищенности, методы качественной оценки рисков.

Keywords: information infrastructure, security, information systems, computer networks, security assessment models, security indicators, methods of qualitative risk assessment.

Новые информационные технологии активно внедряются во все сферы деятельности человека. Появление локальных и глобальных сетей предоставило пользователям компьютеров новые возможности оперативного обмена информацией. Если до недавнего времени подобные сети создавались только в специфических и узконаправленных целях, то развитие интернета и аналогичных систем привело к использованию глобальных сетей передачи данных в повседневной жизни практически каждого человека.

По мере развития средств и методов автоматизации процессов обработки информации увеличивается зависимость общества от степени безопасности используемых информационных систем [6].

Нарушение информационной безопасности компьютерных сетей может быть вызвано следующими причинами [2]:

– наличие уязвимостей в операционных системах и приложениях;

– неверная конфигурация аппаратного и программного обеспечения;

– ошибки, допущенные при настройке контроля доступа;

– наличие уязвимых или легко атакуемых сервисов и вредоносного программного обеспечения.

Используя комбинации имеющихся уязвимостей и недостатков в конфигурации сети, злоумышленник, в зависимости от своих целей, может реализовать разнообразные стратегии нападения. Эти стратегии могут быть направлены на различные критические ресурсы сети. Поэтому при проектировании и эксплуатации локальных вычислительных сетей перед проектировщиком возникает задача проверки того, обеспечивают ли планируемые для применения или уже используемые параметры конфигурации сети необходимый уровень защищенности.

На сегодняшний день существует огромное количество методов оценки защищенности локальных вычислительных сетей. Наиболее распространенными являются следующие методы оценки защищенности [4]:

– метод оценки на основе графов защищенности;

– метод оценки на основе нечеткой логики;

– метод оценки рисков.

Рассматриваемая модель включает в себя все перечисленные методы оценки уровня защищенности, а также охватывает множество различных показателей защищенности (ПЗ) и формул, используемых для их расчета [3]. В соответствие с существующими методами оценки защищенности, определение значений отдельных показателей и общая оценка уровня защищенности локальной вычислительной сети может проводиться с использованием как количественных, так и качественных показателей [7]. Например, при использовании количественных показателей, вероятность проведения атаки может выражаться числом в интервале [0,1]. При использовании качественных показателей числовые значения меняются на эквивалентные им понятийные уровни. Каждому понятийному уровню в этом случае будет соответствовать определенный интервал количественных показателей оценки.

В соответствии с порядком вычислений все ПЗ можно разделить на первичные и вторичные.

Первичные ПЗ получаются непосредственно из дерева атак с использованием параметров атакующих действий, атакуемых хостов и анализируемой сети. Вторичные рассчитываются с использованием первичных ПЗ.

Основными являются следующие ПЗ:

– критичность хоста *h (Criticality(h))*;

– уровень критичности атакующего действия, *a (Severity(a))*;

– размер ущерба, вызванного выполнением атакующего действия с учетом уровня критичности атакуемого хоста *(Mortality(a,h))*;

– размер ущерба при выполнении трассы *S* и угрозы *T (Mortality(S))* и *(Mortality(T))*;

– «сложность в доступе» для атакующего действия, трассы и угрозы *(AccessComplexity(a), AccessComplexity(S), AccessComplexity(T))*;

– степень возможности реализации угрозы *T (Realization(T))*;

– уровень риска угрозы *T (RiskLevel(T))*;

– уровень защищенности компьютерной сети *(SecurityLevel)*.

Показатели защищенности рассчитываются на базе общей системы оценки уязвимостей *(CVSS)* [5].

Множество базовых индексов отражает фундаментальные свойства уязвимостей и состоит из семи индексов:

– вектор доступа *(Access Vector)* – «Локальный» (для использования уязвимости необходим локальный доступ) и «Удаленный» (для использования уязвимости необходим удаленный доступ);

– сложность доступа *(Access Complexity)* – «Высокий» (существуют условия на доступ, например, специфические временные рамки, специфические обстоятельства (специфическая конфигурация сервиса), взаимодействие с атакуемым человеком), «Низкий» (нет специфических условий на доступ);

– необходимость аутентификации *(Authentication)* – «Требуемый» (аутентификация необходима), «Не требуемый» (для реализации атаки аутентификация не нужна);

– воздействие на конфиденциальность *(Confidentiality Impact)* – «Нет» (нет воздействия на конфиденциальность), «Частичный» (значительное раскрытие информации), «Полный» (полное раскрытие критичной информации);

– воздействие на целостность *(Integrity Impact)* – аналогично с предыдущим пунктом – «Нет», «Частичный», «Полный»;

– воздействие на доступность *(Availability Impact)* – аналогично с предыдущим пунктом – «Нет», «Частичный», «Полный»;

– коэффициент уклона воздействия *(Impact Bias)* – «Обычный» (конфиденциальности, целостности и доступности присвоен одинаковый вес), «Конфиденциальность» (больший вес присваивается конфиденциальности), «Целостность» (больший вес присваивается целостности), «Доступность» (больший вес присваивается доступности).

Обобщенная оценка критичности уязвимости рассчитываются по следующей формуле:

$$BaseScore=round(10\cdot AV\cdot AC\cdot A\cdot(CI\cdot IB^{C}+II\cdot IB^{I}+AI\cdot IB^{A})) \quad (1)$$

где *round()* – функция округления до десятых;

$$AV=\begin{cases} 0.7,\ AccessVector=Локальный, \\ 1.0,\ AccessVector=Удаленный, \end{cases} \quad (2)$$

где *AccessVector* – индекс *CVSS* «вектор доступа»;

$$AC=\begin{cases} 0.8,\ AccessComplexity=Высокий, \\ 1.0,\ AccessComplexity=Низкий, \end{cases} \quad (3)$$

где *AccessComplexity* – индекс *CVSS* «сложность доступа»;

$$A=\begin{cases} 0.6,\ Authentication=Требуемый, \\ 1.0,\ Authentication=Не\ требуемый, \end{cases} \quad (4)$$

где *Authentication* – индекс *CVSS* «необходимость аутентификации»;

$$CI=\begin{cases} 0,\ ConfidentialityImpact=Нет, \\ 0.7,\ ConfidentialityImpact=Частичный, \\ 1.0,\ ConfidentialityImpact=Полный, \end{cases} \quad (5)$$

где *ConfidentialityImpact* – индекс *CVSS* «Воздействие на конфиденциальность»;

$$IB^{C}=\begin{cases} 0{,}333,ImpactBias=Обычный, \\ 0{,}5,ImpactBias=Конфиденциальность, \\ 0.25,ImpactBias=Целостность, \\ 0.25,ImpactBias=Доступность, \end{cases} \quad (6)$$

где *ImpactBias* – индекс *CVSS* «коэффициент уклона воздействия»;

$$II=\begin{cases} 0,\ IntegrityImpact=Нет, \\ 0.7,\ IntegrityImpact=Частичный, \\ 1.0,\ IntegrityImpact=Полный, \end{cases} \quad (7)$$

где *IntegrityImpact* – индекс *CVSS* «Воздействие на целостность»;

$$IB^{I}=\begin{cases} 0{,}333,ImpactBias=Обычный, \\ 0{,}5,ImpactBias=Конфиденциальность, \\ 0.25,ImpactBias=Целостность, \\ 0.25,ImpactBias=Доступность, \end{cases} \quad (8)$$

где *ImpactBias* – индекс *CVSS* «коэффициент уклона воздействия»;

$$AI=\begin{cases} 0,\ AvailabilityImpact=Нет, \\ 0.7,\ AvailabilityImpact=Частичный, \\ 1.0,\ AvailabilityImpact=Полный, \end{cases} \quad (9)$$

где *AvailabilityImpact* – индекс *CVSS* «Воздействие на доступность»

$$IB^A=\begin{cases} 0,333, ImpactBias=Обычный, \\ 0,5, ImpactBias=Конфиденциальность, \\ 0.25, ImpactBias=Целостность, \\ 0.25, ImpactBias=Доступность, \end{cases} \quad (10)$$

где *ImpactBias* – индекс *CVSS* «коэффициент уклона воздействия»;

Таким образом, критичность атакующего действия *Severty(a),* рассчитанная с использованием обобщенной оценки критичности уязвимости, делится на три состояния:

$$Severity(a)=\begin{cases} Низкий,\ если\ BaseScore(a)\in[0,0;4,0), \\ Средний,\ если\ BaseScore(a)\in[4,0;7,0), \\ Высокий,\ если\ BaseScore(a)\in[7,0;10,0]. \end{cases} \quad (11)$$

Размер ущерба *Mortality(a,h)*, вызванного успешным выполнением атакующего действия с учетом уровня критичности атакуемого хоста, рассчитывается с помощью матрицы рисков методики анализа и оценки рисков (*FRAAP*) [1]. Данная матрица приведена в таблице 1.

Таблица 1

Определение размера ущерба *Mortality(a,h)*, вызванного успешным выполнением атакующего действия

Критичность хоста *Criticality(h)*	Уровень критичности атакующего действия *Severity(a)*		
	«Высокий»	«Средний»	«Низкий»
«Высокий»	«Высокий»	«Высокий»	«Средний»
«Средний»	«Высокий»	«Средний»	«Низкий»
«Низкий»	«Средний»	«Низкий»	«Низкий»

Критичность хоста *Criticality(h)* определяется проектировщиком экспертным путем, исходя из назначения данного хоста и выполняемых им функций.

Размер ущерба для хоста *h* с учетом его критичности, вызванного успешной реализацией угрозы, определяется ее последним атакующим действием:

$$Mortality\ (T) = Mortality\ (a_T, h_T), \quad (12)$$

где a_T – последнее атакующее действие в угрозе;

h_T – хост, на который направлено действие a_T.

Размер ущерба *Mortality(T)* при реализации угрозы *T* можно охарактеризовать следующим образом:

– «Высокий» – остановка критически важных бизнес-подразделений, которая приводит к существенному ущербу для бизнеса, потере имиджа или неполучению существенной прибыли;

– «Средний» – кратковременное прерывание работы критических процессов или систем, которое приводит к ограниченным финансовым потерям в одном бизнес-подразделении;

– «Низкий» – перерыв в работе, не вызывающий ощутимых финансовых потерь.

Средняя величина уровня критичности $Severity(a)_R$ рассчитывается по формуле:

$$BaseScore_R = \sum_{V_R^{diff}} \frac{BaseScore(a)}{N_R^V} \quad (13)$$

где *BaseScore(a)* – обобщенная оценка критичности уязвимости;

N_R^V – количество различных атакующих действий в рассматриваемой сети;

V_R^{diff} – множество различных атакующих действий.

Сложность доступа ко всей системе в целом $AccessComplexity_R$ рассчитывается по формуле:

$$AccessComplexity_R = \sum_{V_R^{diff}} \frac{AccessComplexity}{N_R^V} \quad (14)$$

где *AccessComplexity* – сложность доступа к отдельному хосту;

N_R^V – количество различных атакующих действий в рассматриваемой сети;

V_R^{diff} – множество различных атакующих действий.

Для получения качественной оценки уровня риска угрозы необходимо оценить степень возможности ее реализации *Realization(T)* (см. формулу 15) и воспользоваться матрицей риска из методики FRAAP с использованием размера ущерба при реализации угрозы *Mortality(T)* (см. таблицу 1). Для определения степени возможности реализации угрозы *T* воспользуемся индексом *CVSS* «Сложность в доступе», задаваемым для каждого атакующего действия (см. формулу 3). Тогда степень возможности реализации угрозы *T* будет рассчитываться по следующей формуле:

$$Realization(T)=\begin{cases}Высокий,\ если\ AccessComplexity(T)=Низкий,\\ Низкий,\ если\ AccessComplexity(T)=Высокий,\end{cases} \quad (15)$$

Оценка уровня риска угрозы получается в соответствие с матрицей риска, базирующейся на соответствующей матрице методики *FRAAP* [1] и представленной в таблице 2.

Таблица 2

Матрица оценки уровня риска угрозы

Степень возможности реализации угрозы	Уровень критичности угрозы (*Severity(T)*)		
	«Высокий»	«Средний»	«Низкий»
«Высокий»	А	Б	В
«Низкий»	В	В	Г

Полученная оценка уровня риска интерпретируется следующим образом:

– А – связанные с риском действия (например, внедрение новых средств защиты информации или устранение уязвимостей) должны быть выполнены немедленно и в обязательном порядке;

– Б – связанные с риском действия должны быть предприняты;

– В – требуется мониторинг ситуации (но непосредственных мер по противодействию угрозе возможно не предпринимать);

– Г – никаких действий в данный момент предпринимать не требуется.

Исходя из полученных качественных оценок уровня риска для всех угроз, определим уровень защищенности анализируемой компьютерной сети следующим образом:

$$SecurityLevel=\begin{cases}Зеленый,\ если\ \forall i\epsilon N,\ i\le N_T,\ RiskLevel(T_i)=Г,\\ Жёлтый,\ если\ \forall i\epsilon N,\ i\le N_T,\ RiskLevel(T_i)\le В,\\ Оранжевый,\ если\ \forall i\epsilon N,\ i\le N_T,\ RiskLevel(T_i)\le Б,\\ Красный,\ если\ \exists i\epsilon N,\ i\le N_T,\ RiskLevel(T_i)=А,\end{cases} \quad (16)$$

где $Г<В<Б<А$

N_T – количество всех угроз.

Согласно методике, *FRAAP* [1] состояния описываются следующим образом:

– *SecurityLevel* = «Зеленый» – никаких действий, направленных на повышение уровня защищенности сети предпринимать не требуется;

– *SecurityLevel* = «Желтый» – требуется мониторинг ситуации;

– *SecurityLevel* = «Оранжевый» – должны быть предприняты действия по повышению уровня защищенности компьютерной сети;

– *SecurityLevel* = «Красный» – действия должны быть предприняты в обязательном порядке.

Рассмотрим небольшую локальную вычислительную сеть, представленную на рисунке 1, и проведём оценку её защищенности. Данная сеть состоит из четырех автоматизированных рабочих мест (АРМ), одного сервера и одного коммутатора.

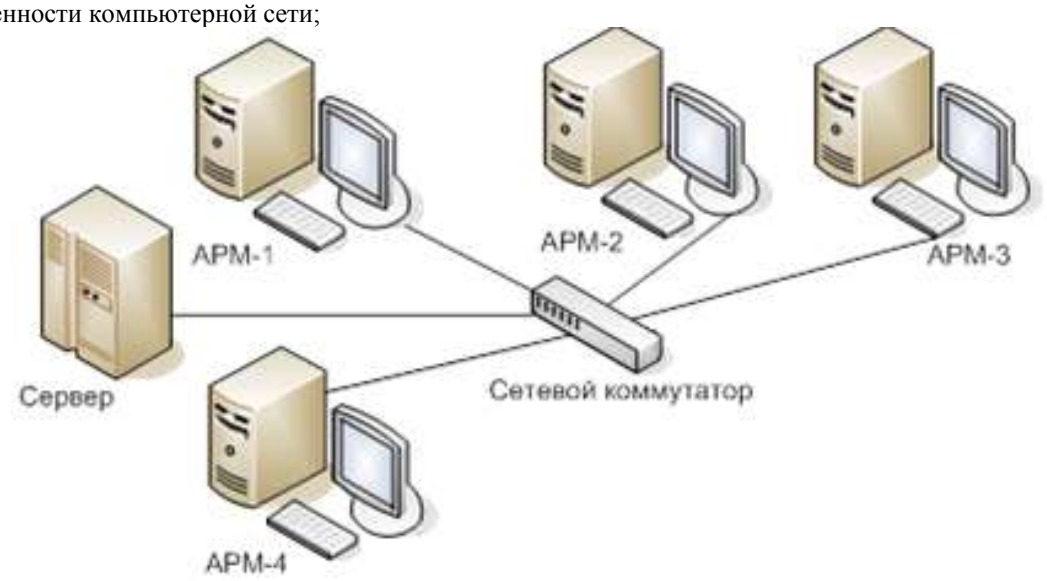

Рисунок 1. Топология оцениваемой локальной вычислительной сети

Используя формулу для расчета обобщенного индекса критичности уязвимости *BaseScore*, получим значения критичности атакующего действия *Severity(a)*, представленные в таблице 3.

Таблица 3

Расчет обобщенного индекса критичности атакующего действия

Наименование хоста	Базовые индексы (согласно CVSS)							Обобщенный индекс критичности уязвимости *BaseScore*	Критичность атакующего действия *Severity(a)*
	AV	*AC*	*A*	*CI*	*II*	*AI*	*IB*		
Сетевой коммутатор	0.7	0.8	0.6	0.7	0.7	0.7	0.333	2.3	«Низкий»
Сервер	0.7	0.8	0.6	0.7	0.7	0.7	0.333	2.3	«Низкий»
АРМ-1	1.0	0.8	0.6	1.0	1.0	1.0	0.333	4.8	«Средний»
АРМ-2	1.0	0.8	0.6	1.0	1.0	1.0	0.333	4.8	«Средний»
АРМ-3	1.0	1.0	1.0	1.0	1.0	1.0	0.333	10.0	«Высокий»
АРМ-4	1.0	1.0	1.0	1.0	1.0	1.0	0.333	10.0	«Высокий»

Рассмотрим случай, когда на каждый хост локальной сети направлено одно атакующее действие.

Тогда по формуле 13

$$BaseScore_R = \frac{2.3+2.3+4.8+4.8+10.0+10.0}{6} = 5.7$$

Таким образом, средняя величина базового индекса *BaseScore* равная *5.7* говорит о «Среднем» уровне критичности атакующих действий на локальную вычислительную сеть (см. формулу 11).

Экспертным путем определим показатели критичности хостов рассматриваемой сети. Результаты представлены в таблице 4.

Таблица 4

Определение критичности хостов

Наименование хоста	Показатель критичности *Severity(h)*
Сетевой коммутатор	«Высокий»
Сервер	«Средний»
АРМ-1	«Низкий»
АРМ-2	«Низкий»
АРМ-3	«Низкий»
АРМ-4	«Низкий»

Теперь, когда нам известны показатель критичности хоста (см. таблицу 4) и показатель критичности атакующего действия (см. таблицу 3), определим размер ущерба *Mortality* (a_T, h_T), вызванного успешным выполнением атакующего действия по таблице 1. Результаты расчёта приведены в таблице 5.

Таблица 5

Определение размера ущерба *Mortality* (a_T, h_T), вызванного успешным выполнением атакующего действия

Наименование хоста	Размер ущерба *Mortality* (a_T, h_T)
Сетевой коммутатор	«Средний»
Сервер	«Низкий»
АРМ-1	«Низкий»
АРМ-2	«Низкий»
АРМ-3	«Средний»
АРМ-4	«Средний»

Определим степень возможности реализации угрозы для каждого хоста (см. формулу 15), для этого воспользуемся индексом *CVSS* «Сложность доступа» (см. формулу 3). Результаты расчета приведены в таблице 6.

Таблица 6

Определение степени возможности реализации угрозы

Наименование хоста	Сложность доступа *(AccessComplexity)*	Значение *AccessComplexity* (см. формула 3)	Степень возможности реализации угрозы *Realization(T)*
Сетевой коммутатор	«Высокий»	0.8	«Низкий»
Сервер	«Высокий»	0.8	«Низкий»
АРМ-1	«Низкий»	1.0	«Высокий»
АРМ-2	«Низкий»	1.0	«Высокий»
АРМ-3	«Низкий»	1.0	«Высокий»
АРМ-4	«Низкий»	1.0	«Высокий»

Определим «Сложность доступа» к локальной вычислительной сети по формуле 14:

$$AccessComplexity_R = \frac{0.8+0.8+1,0+1,0+1.0+1.0}{6} = 0.93$$

Согласно *CVSS* если $AccessComplexity_R \in [0.8; 0.9)$, то уровень сложности доступа – «Высокий», если $AccessComplexity_R \in [0.9; 1,0]$, то уровень сложности доступа – «Низкий».

Таким образом, значение «0.93» показывает, что уровень сложности доступа к сети – «Низкий». Тогда, степень реализации угрозы имеет показатель «Высокий» (см. формула 15).

Теперь определим уровень риска угрозы *RiskLevel(T)* согласно таблице 2. Результаты расчёта приведены в таблице 7.

Таблица 7

Оценка уровня риска угрозы

Степень возможности реализации угрозы *Realization(T)*	Уровень критичности угрозы $Severity(a)_R$	Уровень риска угрозы *RiskLevel(T)*
«Высокий»	«Средний»	«Б»

Таким образом, исходя из полученных качественных оценок уровня риска для всех угроз, уровень защищенности локальной вычислительной сети *SecurityLevel* имеет уровень «Оранжевый». Это означает, что рассматриваемая вычислительная сеть уязвима к атакующим действиям, поэтому необходимо предпринять действия по повышению уровня защищенности.

Для более чёткого понимания того, каким образом можно увеличить уровень защищенности локальной вычислительной сети *SecurityLevel* приведем графики зависимости «Уровня риска угрозы» от количества АРМ, имеющих высокую сложность к доступу. Графики зависимости приведены на рисунках 2–5.

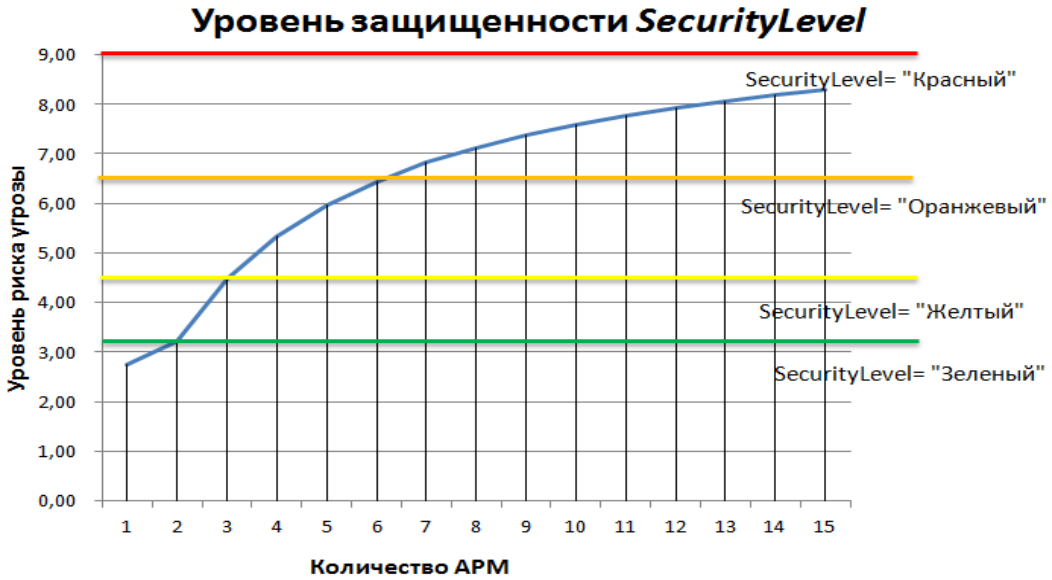

Рисунок 2. Зависимость уровня защищенности локальной вычислительной сети от количества АРМ (сложность доступа – «Низкий»)

Из графика (см. рисунок 2) видно, что в локальной сети, включающей в себя два АРМ уровень защищённости сети будет иметь показатель «Зелёный», при трёх АРМ – «Желтый», при большем количестве АРМ данной сети будет нанесён значительный ущерб.

Рисунок 3. Зависимость уровня защищенности локальной вычислительной сети от количества хостов (АРМ) (сложность доступа – «Высокий»)

Из графика (см. рисунок 3) видно, что в локальной сети, где все АРМ (всего 36 АРМ) имеют высокую сложность в доступе, уровень риска угрозы не превышает *SecuirityLevel*= «Желтый». В данном случае сеть будет достаточно защищена от атакующих действий.

Рисунок 4. Зависимость уровня защищенности локальной вычислительной сети от количества хостов (АРМ) (сложность доступа – «Высокий» у 25% АРМ)

Из графика (см. рисунок 4) видно, что в локальной сети, где 25% АРМ (всего 200 АРМ) имеют высокую сложность в доступе, уровень риска угрозы не превышает *SecuirityLevel*= «Желтый» при количестве АРМ равным 85. При большем количестве АРМ данной сети будет нанесён значительный ущерб.

Рисунок 5. Зависимость уровня защищенности локальной вычислительной сети от количества хостов (АРМ) (сложность доступа – «Высокий» у 40% АРМ)

Из графика (см. рисунок 5) видно, что в локальной сети, где 40% АРМ (всего 200 АРМ) имеют высокую сложность в доступе, уровень риска угрозы не превышает *SecuirityLevel*= «Желтый» при количестве АРМ равным 160. При большем количестве АРМ данной сети будет нанесён значительный ущерб.

Таким образом, при увеличении числа АРМ с высокой сложностью доступа увеличивается и уровень защищенности локальной вычислительной сети.

Для повышения уровня доступа к данным, хранящимся на компьютере, могут использоваться пароли. В таком случае компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль. Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам. При этом может проводиться регистрация всех попыток несанкционированного доступа.

Для стабильного функционирования локальной компьютерной сети необходимо, чтобы «Уровень защищенности *SecurityLevel*» находился на отметке «Зеленый» либо «Желтый», что не позволит злоумышленнику нанести ущерб сети.

Таким образом, алгоритм оценки уровня защищенности локальных вычислительных сетей, включающий в себя систему различных показателей защищенности, позволяет быстро регулировать порог формирования сигнала тревоги, что в свою очередь, позволит с большей эффективностью оценивать их защищенность и более динамично управлять локальной вычислительной сетью.

Список литературы

1. Peltier, T.R. Information security risk analysis, second edition / Taylor&Francis Group, 2005.

2. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак [Электронный ресурс]. – Режим доступа: http://www.isa.ru/proceedings/images/documents/2007-31/126-207.pdf.

3. Дойникова, Е.В. Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов/ Е.В. Дойникова // сб. публикаций научного журнала «Труды СПИИРАН». – 2013. – Вып. 3 (26). – С. 54 – 68.

4. Курочкин, С.И. Методы оценки защищенности информационных систем / С.И. Курочкин, И.В. Заводцев // сб. публикаций научного журнала «Перспективы развития информационных технологий». – 2016. – N29. – С. 197 – 204.

5. Общая система оценки уязвимостей [Электронный ресурс]. – Режим доступа: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

6. Студенческий научный форум - 2018 [Электронный ресурс]. – Режим доступа: https://scienceforum.ru/2018/article/2018003735.

7. Файзуллин, Р.Р. Метод оценки защищенности сети передачи данных в системе мониторинга и управления событиями информационной безопасности на основе нечеткой логики / Р.Р. Файзуллин, В.И. Васильев // сб. публикаций научного журнала «Вестник УГАТУ». – 2013. – Т.17, N2 (55). – С. 150 – 156.