



ОЦЕНКА ЭФФЕКТИВНОСТИ МЕТОДА ЗАЩИТЫ ХРАНИЛИЩА ЗАДАНИЙ ДЛЯ РАСПРЕДЕЛЕННОЙ АСУ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Аннаева Айлар Ражаповна

Преподаватель Международного университета нефти и газа имени Ягшыгелди Какаева,
г. Ашхабад Туркменистан

Атаев Мухамметнур Абдылгапурович

Преподаватель Международного университета нефти и газа имени Ягшыгелди Какаева,
г. Ашхабад Туркменистан

Батыров Ыляс

Студент Международного университета нефти и газа имени Ягшыгелди Какаева,
г. Ашхабад Туркменистан

Довлетгелдиев Сердар

Студент Международного университета нефти и газа имени Ягшыгелди Какаева,
г. Ашхабад Туркменистан

Одной из актуальных информационных угроз является нарушение функционирования промышленного оборудования, вызванного несанкционированным воздействием на объекты корпоративной сети предприятия. Для промышленных производственных предприятий уязвимым узлом является место хранения информации, в котором содержится необходимые данные для работы отраслевого сегмента производства.

В работе [1] отмечается, что обеспечение информационной безопасности АСУ ТП требует системного подхода и вложения ресурсов, вытекающих из необходимости постоянного совершенствования. В условиях современной реальности в связи с устойчивым курсом на импортозамещение, а также на фоне глобальной экономико-политической ситуации, важным шагом становится активное создание и поддержка отечественных систем аппаратно-программных средств и комплексов при построении АСУ ТП, чтобы минимизировать зависимость от стран-производителей популярных операционных систем и компонентов АСУ ТП.

По усреднённым оценкам [2] специалистов CISO/CSO, около 25% инфраструктуры не защищены от сегодняшних угроз безопасности. По мере расширения поверхности атаки устаревшие архитектуры безопасности часто не могут масштабироваться для удовлетворения новых требований устойчивости ИКТ к кибератакам. В ближайшие годы отмечается [3] рост количества атак с использованием новейших технологий для совершения противоправных деяний.

Рост степени информатизации современных предприятий, в том числе и промышленных, обуславливает значительное влияние автоматизированных систем (АС) на их эффективность [4,5]. В связи с этим, существует необходимость в обеспечении информационной безопасности АС.

Особенно это актуально для промышленных предприятий (ПП) полного цикла, для которых угрозы ИБ могут нанести не только значительный финансовый ущерб, но и привести к человеческим жертвам [6] . Увеличение количества инцидентов с информационными системами промышленных предприятий и АСУ ТП за последние годы определяют актуальность их защиты [7,8].

На фоне развития современных средств проникновения разработанный метод защиты хранилища заданий для распределенной АСУ на основе технологии блокчейн является актуальным фактором противодействия нарушения целостности и доступности информации.

Структурная схема функционирования ПО защиты хранилища заданий для распределенной подсистемы АСУ «Sommer» состоит из четырех субъектов участников защиты: блоки данных хранилища заданий; программный комплекс, выполняющий процедуры проверки блоков, вычисления хэш-сумм файлов и управляющий процессом сбора и передачи информации; распределенный реестр, отвечающий за хранение хэш-сумм файлов; центр принятия решений, отвечающий за алгоритм действий при обнаружении аномалий.

Достоинством структурной схемы функционирования ПО защиты хранилища заданий для распределенной подсистемы АСУ в децентрализованном исполнении является оптимальность с точки зрения безопасности [9]. Каждый из функционирующих узлов требует определенной стратегии для проникновения. В случае же успешной атаки будет нанесен ущерб одному или нескольким распределённым ресурсам, что с большой долей вероятности не повлияет отрицательно на работу всей системы одновременно[10]. При внесении несанкционированных изменений в блок данных задания АСУ – программный комплекс при периодической проверки оперативно отследит на каком из устройств произошло вторжение и отключит его от общей сети предприятия на время устранения обнаруженной уязвимости. Внесение изменений в распределенный реестр, построенный на основе технологии блокчейн не влияет на производственный цикл предприятия, поскольку содержит не данных изделий, а только вычисленные хэш значения. Выход из строя самого рабочего места никак не повреждает ни данные реестра, ни хранилища заданий. Поэтому именно децентрализованное исполнение структурной схемы с точки зрения безопасности является оптимальным вариантом исполнения [11].

Модель системы защиты хранилища заданий на основе технологии блокчейн имеет входные и выходные параметры (рисунок 1).



Рисунок 1. Модель системы защиты хранилища заданий

Входные параметры:

N – количество узлов блокчейн;

$P_{\text{отказ}}$ – вероятность отказа узла блокчейн;

$P_{\text{взлома}}$ – вероятность взлома узла;

U – ценность задания/оценка ущерба;

$I_{\text{ср}}$ – средняя нагрузка на сеть от блокчейн на распространение данных между узлами;

$V_{\text{ср}}$ – дополнительная нагрузка на ПК для расчета хэш в системе блокчейн.

Выходные параметры:

$P_{\text{наруш.дост.}}$ – вероятность потери данных вследствие отказа всех устройств;

$P_{\text{вер.наруш}}$ – вероятность нарушения целостности задания из-за взлома узлов;

I – нагрузка на сеть со стороны блокчейн;

V – общая нагрузка на вычислительную систему;

R – оценка риска.

Вероятность нарушения доступности рассчитывается как

$$P_{\text{наруш.дост.}} = \prod_{i=1}^N P_{\text{отказ}}$$

Для потери всех данных нужно, чтобы все устройства вышли из строя.

Для оценки вероятности нарушения доступности приведем расчетные характеристики в таблице 1.

Таблица 1

Вероятности нарушения доступности

N	$P_{\text{отказ}}=0,4$	$P_{\text{отказ}}=0,5$	$P_{\text{отказ}}=0,6$	$P_{\text{отказ}}=0,7$	$P_{\text{отказ}}=0,8$	$P_{\text{отказ}}=0,9$
1	0,40000	0,50000	0,60000	0,70000	0,80000	0,90000
2	0,16000	0,25000	0,36000	0,49000	0,64000	0,81000
3	0,06400	0,12500	0,21600	0,34300	0,51200	0,72900
4	0,02560	0,06250	0,12960	0,24010	0,40960	0,65610
5	0,01024	0,03125	0,07776	0,16807	0,32768	0,59049
6	0,00410	0,01563	0,04666	0,11765	0,26214	0,53144
7	0,00164	0,00781	0,02799	0,08235	0,20972	0,47830
8	0,00066	0,00391	0,01680	0,05765	0,16777	0,43047
9	0,00026	0,00195	0,01008	0,04035	0,13422	0,38742
10	0,00010	0,00098	0,00605	0,02825	0,10737	0,34868

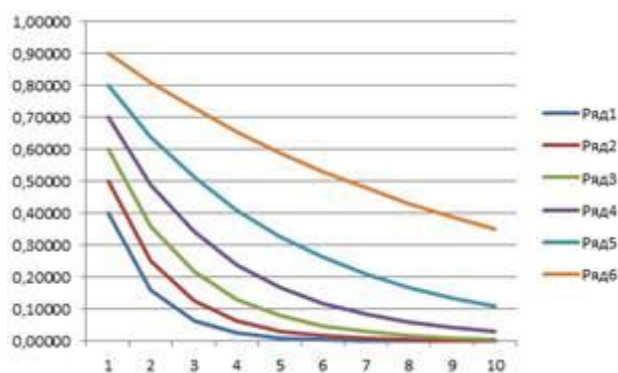


Рисунок 2. График зависимости вероятности нарушения доступности в зависимости от количества узлов N

Можно сделать вывод, что для вероятности выше 0,6 оптимальным количеством узлов обеспечивающих доступность данных является $N=7$.

Вероятность нарушения целостности определяется как

$$P_{\text{наруш.целост.}} = \prod_{i=1}^{\frac{N}{2}+1} P_{\text{взлома}}$$

Для оценки вероятности нарушения целостности приведем расчетные характеристики в таблице 2.

Таблица 2

Вероятности нарушения целостности

	$P_{\text{взл}}=0,4$	$P_{\text{вз}}=0,5$	$P_{\text{вз}}=0,6$	$P_{\text{вз}}=0,7$	$P_{\text{вз}}=0,8$	$P_{\text{вз}}=0,9$
1	0,25298	0,50000	0,46476	0,58566	0,71554	0,85381
2	0,16000	0,25000	0,36000	0,49000	0,64000	0,81000
3	0,10119	0,17678	0,27885	0,40996	0,57243	0,76843
4	0,06400	0,12500	0,21600	0,34300	0,51200	0,72900
5	0,04048	0,08839	0,16731	0,28697	0,45795	0,69159
6	0,02560	0,06250	0,12960	0,24010	0,40960	0,65610
7	0,01619	0,04419	0,10039	0,20088	0,36636	0,62243
8	0,01024	0,03125	0,07776	0,16807	0,32768	0,59049
9	0,00648	0,02210	0,06023	0,14062	0,29309	0,56019
10	0,00410	0,01563	0,04666	0,11765	0,26214	0,53144

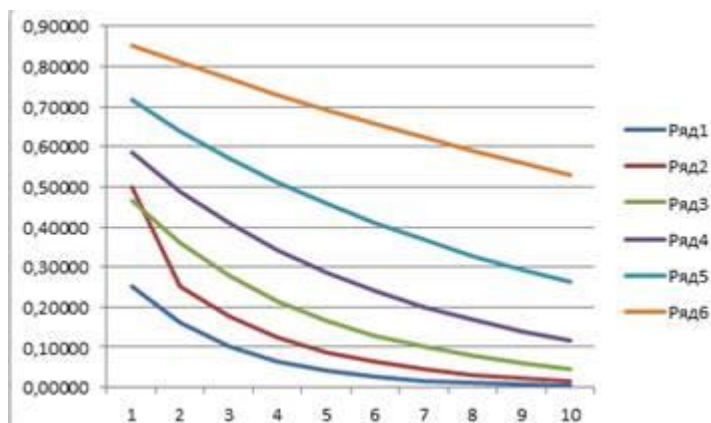


Рисунок 3. График вероятности нарушения доступности в зависимости от количества узлов N

Можно сделать вывод, что для вероятности выше 0,6 минимальным количеством узлов обеспечивающих целостность данных является N=10.

Нагрузка на сеть со стороны блокчейн будет определяться как

$$I = I_{\text{ср}} * N.$$

Расчетным путём установлено, что нагрузка на сеть, общий объем передачи данных равен 125Мб, при среднем количестве блоков равным 5000, при среднем размере блока равным 25 кб., что соответствует 1,3% загруженности сети.

Таким образом, при N=10

$$I = 1,3\% * 10 = 13\%$$

Нагрузка сетевых ресурсов увеличится на 13%.

Общая нагрузка на вычислительную систему при средней загруженности вычисления 0,4% для N=10 составит:

$$B = 0,4 * 10 = 4\%$$

Оценка риска для N=10 и U=0.15 для вероятности возникновения инцидента 0,5 в таком случае составит:

$$R = 0,00098 * 0,15 + 0,01563 * 0,15 = 0,00249$$

Таким образом, суммарный риск при N=10 составит 0,249%.

Из приведенных расчетов количество распределенных узлов обеспечивающих необходимый допустимый уровень вероятности нарушения доступности и целостности равен 10. В реализованной системе защиты хранилища заданий на текущий момент времени установлено 16 распределенных узлов содержащих информационные параметры, что значительно превышает расчетные характеристики и обеспечивает требуемые вычислительные мощности распределенной системы.

Расчетная вычислительная нагрузка на сетевые ресурсы и аппаратные ресурсы не представляет никаких существенных затрат для всей инфраструктуры распределённой автоматизированной системы.