CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org

Volume: 03 Issue: 10 | Oct 2022 ISSN: 2660-5309

МОДЕЛИРОВАНИЕ ПРОЦЕССА DDoS-АТАКИ НА БАНКОВСКИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Бекбаев Гамзатдин Алеуатдинович
Кандидат Технических Наук, И.О.Доцент Кафедры "Общественно-Гуманитарные И Точные Науки" Ташкентского Государственного Экономического Университета
e-mail: gamzat--86@mail.ru

АННОТАЦИЯ

В условиях цифровой экономики система расчетов между банками и автоматизации их работы на рынке ценных бумаг, розничных операций (работа банкоматов, терминалов и кредитных карточек), системы автоматизированного взаимодействия является важной функцией банков. Банки уделяют пристальное внимание к работе с клиентами через такие программы как «банк-клиент», совершенствуется обмен информацией с филиалами и отделениями расположенных в других городах, а связь с ними обеспечивается с помощью банковских информационных систем (БИС). За последние месяцы текущего года были выявлены несколько кибератаки на банковские информационные системы крупнейших банков республики. В частности на БИС "Асакабанк" [1], "InfinBank" [2] и "Давр банк" [3]. В результате кибератак хакеры (злоумышленники) присвоили несколько миллиардов сумов. Таким образом, актуализируется задача научной оценки возможностей нарушителя по осуществлению кибератак на сетевые элементы БИС банковских сфер Республики Узбекистан. В настоящей статье рассматривается модель процесса реализации DDoS-атаки на сетевые элементы БИС и приведен расчетный пример. Модель позволяет оценить возможности и действия нарушителя, время затрачиваемое им на реализацию DDoS-атаки на сетевые элементы и вычислить коэффициент исправного действия сетевого элемента при реализации кибератаки.

ARTICLEINFO

Article history:
Received 19 Aug 2022
Revised form 18 Sep 2022
Accepted 22 Oct 2022

Ключевые слова: *банковская информационная система, кибератака, DDoS-атака, топологическое преобразование стохастических сетей.*

---***---

ВВЕДЕНИЕ

В условиях цифровой экономики для обеспечения максимальной эффективности деятельности банковских сфер, в его информационной инфраструктуре применяются современные инфокоммуникационные технологии, а также автоматизированные системы обработки информации и управления, которые обрабатывают информацию о состоянии реализуемого технологического процесса и обеспечивают сохранение конфиденциальности информации, касающейся банковских учетов, персональных данных или коммерческой тайны клиентов. Вместе с неоспоримыми преимуществами применения современных инфокоммуникационных технологий, возросли риски, обусловленные реализацией нарушителем угроз кибератаки, которые могут привести не только к утрате конфиденциальности или потере данные, но и нарушению функционирования банковских информационных систем.

Как показал научный анализ [4-6], разовая реализация организационно-технических мероприятий по кибербезопасности не может обеспечить надежной защиты от угроз кибератаки в течение продолжительного функционирования. Это связано с постоянным развитием информационных технологий, совершенствованием методов и способов реализации кибератак, используемых нарушителем, целью которого является нарушение банковских операций. На сегодняшний день в области информационной безопасности известно более десяти тысяч различных видов компьютерных атак. В опубликованных научных трудах [5-9] подробно изложены основные виды кибератак. Как следует из проведенного в [4-8] анализа, в настоящее время, наиболее «эффективной» является атака с «распределенным отказом в обслуживании» (Distributed Denial of Service, DDoS). При реализации DDoS-атаки нарушитель сначала реализует «взламывание» множества сетевых компьютеров (хостов) для запуска на них заранее установленных программных закладок, обеспечивающих возможность реализации атак «отказ в обслуживании» (Denial of Service, DoS), а затем осуществляет согласованные во времени атаки на целевой хост. Широкое использование нарушителем данного типа компьютерных атак обусловлено их простотой, малой себестоимостью, отсутствием необходимости в специальной подготовке и глубоком знании языков программирования и информационных технологий. Компьютерные атаки обладают вероятностно-временными характеристиками (ВВХ), определение которых позволяет оценить степень их опасности, обоснованно выбрать и реализовать меры защиты. Для исследования и определения ВВХ компьютерных атак необходима разработка их моделей, с этой целью в работе предложена профильная модель DDoS-атаки на сетевые элементы БИС.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОЦЕССА ВОЗДЕЙСТВИЯ

DDoS–АТАКИ НА СЕТЕВЫЕ ЭЛЕМЕНТЫ БИС

С технической точки зрения ИБС включают в себя – маршрутизаторы, коммутаторы, серверы, модемы и автоматизированные рабочие места (АРМ). Предположим, что сетевые элементы ИБС функционируют в условиях DDoS-атак организованного нарушителя. Под организованным нарушителем (злоумышленником) понимается группа людей, состоящая из высококвалифицированных специалистов в области информационной безопасности (ИБ), действующая по единому, согласованному во времени и месту плану и замыслу с целью нанесения ущерба ИБС. На рисунке-1 представлен принцип организации DDoS-атаки на сетевые элементы ИБС. DDoS-атака основана на реализации множества отдельных DoS-атак за счет контроля нарушителем серверов, в которые нарушителем заблаговременно внедрены специальные программы агенты [5-10].

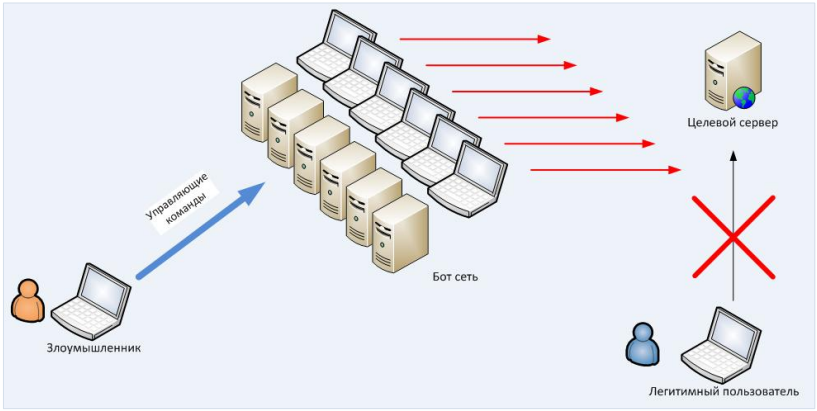

Рис.1. Принцип реализации типовой DDoS-атаки на сетевые элементы ИБС

При поступлении команды от компьютера нарушителя, множество «зомби-компьютеров» обращаются с запросами к серверу, заставляя его реагировать на них, а эти «зомби-компьютеры» образуют «бот-сеть», то есть сеть зараженных узлов, которой управляет нарушитель. В результате, бот-сеть начинает обращаться с какими-либо запросами к целевой системе блокируя возможность ответа легитимным пользователям. DDoS-атака считается успешной, если она привела к недоступности информационного ресурса для легитимных пользователей банка.

Для успешной реализации DDoS-атаки организованный нарушитель реализует следующие частные процессы, аналогично как в работе [5-10], кроме того, с вероятностью $(1-P_{\text{отп.запр}})$ на атакуемые сервера может быть направлен некорректный, специально подобранный запрос за некоторое время $\overline{t}_{\text{нек.запр}}$ с функцией распределения $O(t)$. В этом случае, при наличии ошибок в удаленной системе, возможно зацикливание процедуры обработки запроса, переполнение буфера с последующим «зависанием» сервера. Требуется определить интегральную функцию распределения вероятностей $F(t)$, среднее время $\overline{T}_p$ и коэффициент исправного действия сервера при реализации нарушителем DDoS-атаки.

При моделировании вводятся следующие ограничения и допущения:

- возможности организованного нарушителя по доступу к элементам ИБС, характеризуются указанными в постановке задачи вероятностными показателями;
- законы распределения случайного времени реализации частных процессов относится к классу экспоненциальных;
- значения вероятностей полагаются одинаковыми, т.е. $P_{\text{оп.элем}} = P_{\text{оп.ос}} = P_{\text{оп.серв}} = P_{\text{отп.запр}} = P_{\text{под.с}} = P_{\text{п}}$.

Решение:

Описанный в постановке задачи процесс реализации DDoS-атаки на сетевые элементы ИБС представим в виде стохастической сети, приведенной на рисунке 2.

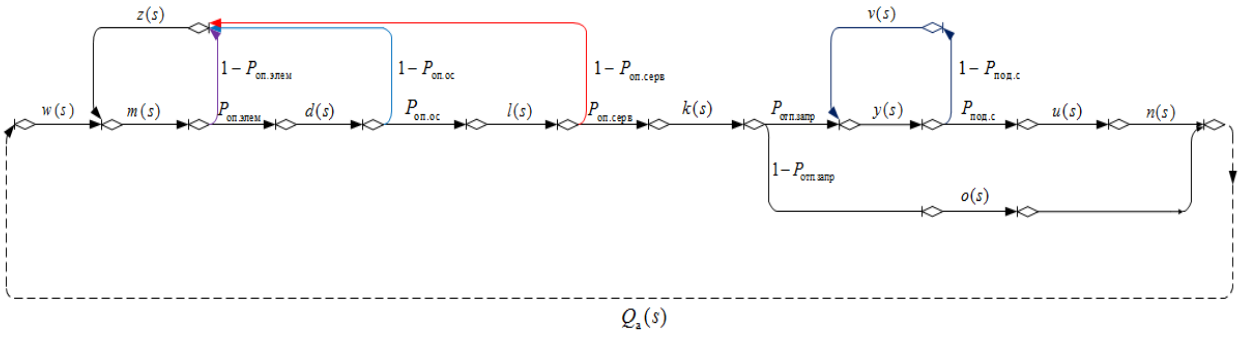

Рис.2. Стохастическая сеть процесса реализации DDoS-атак сетевые элементы ИБС

В стохастической сети обозначено: $w(s)$, $m(s)$, $z(s)$, $d(s)$, $l(s)$, $k(s)$, $y(s)$, $o(s)$, $v(s)$, $u(s)$ и $n(s)$ – преобразования Лапласа-Стилтьеса соответствующих функций распределения, указанных в постановке задачи и определяемых как (1):

$$r_i(s) = \int_0^{\infty} \exp(-st) d[R_i(t)] = \frac{r_i}{r_i + s} \qquad (1)$$

С целью определения эквивалентной функции стохастической сети (рис.2) замкнем вход и выход стохастической сети фиктивной ветвью $Q_a(s) = \frac{1}{Q(s)}$ и перечислим петли первого и второго порядков [5-11]:

Петли первого порядка:

$\text{loop1}_1 := m(s) \cdot (1 - P_n) \cdot z(s)$;

$\text{loop1}_2 := m(s) \cdot d(s) \cdot P_n \cdot (1 - P_n) \cdot z(s)$;

$\text{loop1}_3 := m(s) \cdot d(s) \cdot l(s) \cdot P_n^2 \cdot (1 - P_n) \cdot z(s)$;

$\text{loop1}_4 := y(s) \cdot (1 - P_n) \cdot v(s)$;

$\text{loop}_{общ1} := w(s) \cdot m(s) \cdot d(s) \cdot l(s) \cdot k(s) \cdot y(s) \cdot u(s) \cdot n(s) \cdot P_n^5$;

$\text{loop}_{общ2} := w(s) \cdot m(s) \cdot d(s) \cdot l(s) \cdot k(s) \cdot o(s) \cdot (1 - P_n) \cdot P_n^3$

Петли второго порядка:

$\text{loop2}_1 := m(s) \cdot (1 - P_n)^2 \cdot z(s) \cdot y(s) \cdot v(s)$;

$\text{loop2}_2 := m(s) \cdot d(s) \cdot P_n \cdot (1 - P_n)^2 \cdot z(s) \cdot y(s) \cdot v(s)$;

$\text{loop2}_3 := m(s) \cdot d(s) \cdot l(s) \cdot P_n^2 \cdot (1 - P_n)^2 \cdot z(s) \cdot y(s) \cdot v(s)$.

С использованием уравнения Мейсона $H = 1 + \sum_{i=1}^{k} (-1)^k \cdot Q_k(s) = 0$, где $Q_k(s)$ - эквивалентные функции петель k-го порядка, определим эквивалентную функцию стохастической сети (2):

$$Q(s, P_n) = \frac{w(s) \cdot m(s) \cdot d(s) \cdot l(s) \cdot k(s) \cdot y(s) \cdot u(s) \cdot n(s) \cdot P_n^5}{1 - m(s) \cdot (1 - P_n) \cdot z(s) \cdot \left[1 + d(s) \cdot P_n + d(s) \cdot l(s) \cdot P_n^2\right] - y(s) \cdot (1 - P_n) \cdot v(s) +}$$

$$\frac{}{+ m(s) \cdot (1 - P_n)^2 \cdot z(s) \cdot y(s) \cdot v(s) \cdot \left[1 + d(s) \cdot P_n + d(s) \cdot l(s) \cdot P_n^2\right]} + \frac{w(s) \cdot m(s) \cdot d(s) \cdot l(s) \cdot k(s) \cdot o(s) \cdot (1 - P_n) \cdot P_n^3}{1 - m(s) \cdot (1 - P_n) \cdot z(s) \cdot \left[1 + d(s) \cdot P_n + d(s) \cdot l(s) \cdot P_n^2\right]} \qquad (2)$$

Так как (2), по определению, является характеристической функцией, то ее дифференцирование позволяет найти первый и второй начальные моменты случайного времени реализации моделируемого процесса, т.е.

$$M_1(s,P_{\text{п}}) = -\frac{d}{ds}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0},$$

$$M_2(s,P_{\text{п}}) = \frac{d^2}{ds^2}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0}$$

Отсюда среднее время реализации DDoS-атаки равно

$$\overline{t}_{\text{р}}(P_{\text{п}}) = -\frac{d}{ds}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0}$$

Дисперсия времени реализации DDoS-атаки $D(\overline{t}_{\text{р}})$, определяемая как второй центральный момент, представлена выражением

$$D(\overline{t}_{\text{р}}) = \frac{d^2}{ds^2}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0} - \left\{-\frac{d}{ds}\left[\frac{Q(s,P_{\text{п}})}{Q(s=0,P_{\text{п}})}\right]_{s=0}\right\}^2$$

Вычисление математического ожидания и дисперсии позволяет с достаточной для инженерных расчетов точностью определить интегральную функцию распределения времени успешной реализации DDoS-атаки, как неполную Гамма-функцию [10]:

$$F(t) = \begin{cases} 0, \text{ если } t < 0; \\ \int_0^t \frac{\mu^{\alpha}}{\Gamma(\alpha)} \cdot t^{\alpha-1} \cdot e^{-\mu \cdot t} dt, \text{ если } t > 0 \end{cases}, \quad (3)$$

где $\alpha = \frac{[\overline{t}_{\text{р}}(P_{\text{п}})]^2}{D(\overline{t}_{\text{р}})}$ - параметр формы; $\mu = \frac{\overline{t}_{\text{р}}(P_{\text{п}})}{D(\overline{t}_{\text{р}})}$ - параметр масштаба.

РЕЗУЛЬТАТЫ

Расчеты производились с использованием программного комплекса MathCAD-2014. По формуле (3) произведены расчеты, результаты которых представлены на рисунке 3. В качестве исходных данных использовались следующие значения среднего времени реализации частных процессов: $\overline{t}_{\text{зап}} = 2\,\text{мин.}$, $\overline{t}_{\text{оп.элем}} = 7\,\text{мин.}$, $\overline{t}_{\text{оп.ос}} = 5\,\text{мин.}$, $\overline{t}_{\text{оп.серв}} = 6\,\text{мин.}$, $\overline{t}_{\text{оп.уязв}} = 7\,\text{мин.}$, $\overline{t}_{\text{повт.ск}} = 4\,\text{мин.}$, $\overline{t}_{\text{запр}} = 4\ \text{мин.}$, $\overline{t}_{\text{дос.к серв.}} = 1\,\text{мин.}$, $\overline{t}_{\text{пов.запр}} = 4\,\text{мин.}$, $\overline{t}_{\text{завис}} = 3\,\text{мин.}$, $\overline{t}_{\text{нек.запр}} = 3\,\text{мин.}$ а значения вероятностей изменялось в пределах $P_{\text{п}} = 0,7 \div 0,9$.

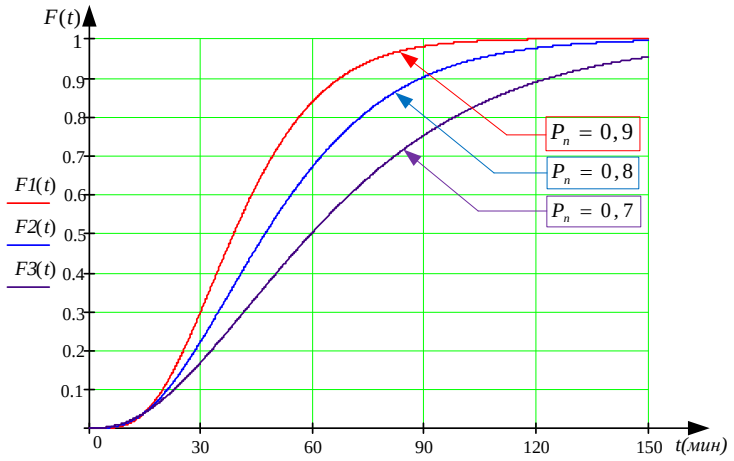

Рис.3. Зависимость интегральной функции распределения вероятностей от времени реализации DDoS-атаки при успешной реализации с вероятностью $P_{\text{п}}$

В свою очередь, среднее время реализации DDoS-атаки при различных значениях $P_{\text{п}}$ составляет: при $P_{\text{п}} = 0,7$, $\overline{T}_p = 64,445$ *мин.*; при $P_{\text{п}} = 0,8$, $\overline{T}_p = 50,197$ *мин.* , а при $P_{\text{п}} = 0,9$ $\overline{T}_p = 41,129$ *мин.*

Коэффициент исправного действия сервера (сетевых элементов) определим как (4):

$$K_{и.д.серв}(t) = \frac{T_И(t)}{T_И(t) + T_B}, \qquad (4)$$

где: $T_И(t) = \dfrac{1-F(t)}{f(t)} = \dfrac{1-\int_0^t \dfrac{\mu^\alpha}{\Gamma(\alpha)} \cdot t^{\alpha-1} \cdot e^{-\mu \cdot t} dt}{\dfrac{\mu^\alpha}{\Gamma(\alpha)} \cdot t^{\alpha-1} \cdot e^{-\mu \cdot t}}$ – среднее время исправной работы; $T_B = 0,5$ *ч* среднее время восстановления сервера (сетевых элементов) после отказа, согласно [5-8].

Изменение коэффициента исправного действия сервера при $T_B = 0,5$ *ч* и различных значениях вероятности $P_{\text{п}}$ показана рисунке 4.

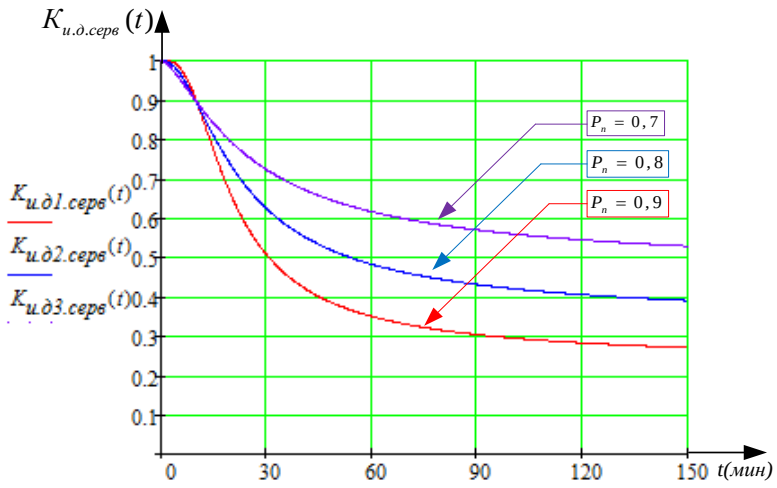

Рис.4. График коэффициента исправного действия серверапри различных значениях вероятности $P_{\text{п}}$

ВЫВОДЫ И ПРЕДЛОЖЕНИЯ

Анализ полученных результатов позволяет сделать следующие выводы:

- разработанная модель является работоспособной, чувствительной к изменению исходных данных, адекватно отображает процесс реализации DDoS-атак и дает возможность определить вероятностно-временные характеристики системы кибервоздействия нарушителя;
- полученные результаты могут быть использованы в ходе комплексной оценки устойчивости функционирования сетевых элементов ИБС;
- особенностью представленной модели является то, что она является укрупненной и учитывает полученные ранее результаты моделирования процессов сканирования портов и идентификации сервисов, определения типа (версии) операционных систем (ОС) и уязвимости узлов [5-10].

Результаты моделирования показывают, что основное влияние на успешность реализации нарушителем DDoS-атаки на сетевые элементы ИБС оказывают параметры, отображающие его доступность к сетевым элементам, применяемые в ИБС методы идентификации и аутентификации легитимных пользователей, а также уровень подготовки (квалификации) нарушителя. Для повышения защищенности сетевых элементов ИБС от DDoS-атак целесообразно использовать организационно-технических мероприятий, изложенные в работах [5-8, 11-15]:

1. Специализированное программно-аппаратное обеспечение.

Следует отметить, что DDoS-атака может быть реализована практически на любом уровне ISO/OSI, однако особой «популярностью» пользуются атаки на 3-4 и 7 уровнях модели. DDoS-атаки на 3-м и 4-м уровне ISO/OSI представляют собой нападение на элементы инфраструктуры сети, основанное на передаче большого объема данных (flood) на транспортном уровне инфраструктуры сети с целью замедления (блокирования) работы web-сервера, загрузки каналов доступа и, в конечном счете, блокирования доступа легитимных пользователей к предоставляемым сетью услугам (ресурсам). Как правило, указанные атаки включают в себя ICMP, SYN и UDP flood. Для защиты от DDoS-атак на 4-7 уровнях используется – экраны, ограничения сеанса, SYN cookie, а на 3-4 уровнях – линейные списки контроля доступа, ограничение скорости.

В случае DDoS-атаки на 7-й уровень ISO/OSI нападение совершается на сервер приложений, что приводит к его перегрузке и существенно затрудняет исполнение пользователем своих функциональных обязанностей. Данный вид атак, с точки зрения реализации, является особенно сложным и характеризуется высокой скрытностью из-за их сходства с полезным трафиком. Кроме того, они непрерывно совершенствуются путем множественного изменения сигнатур, что существенно затрудняет распознавание и нейтрализацию. На сегодняшний день наиболее часто используется следующие программно-аппаратные средства защиты от DDoS-атак:

- брандмауэры с динамической проверкой пакетов;
- динамические механизмы SYN-прокси;
- ограничение количества SYN-ов за секунду для каждого IP-адреса;
- ограничение количества SYN-ов за секунду для каждого удаленного IP-адреса;
- установка экранов ICMP и UDP flood на брандмауэре;
- ограничение скорости роутеров, примыкающих к брандмауэрам и сети.

2. Фильтрация. Фильтрация и блокировка трафика, исходящего от атакующих машин позволяет снизить или вовсе нейтрализовать атаку. При использовании этого метода входящий трафик фильтруется в соответствии с теми или иными правилами, заданными при установке фильтров.

Можно выделить два способа фильтрации: маршрутизация по спискам ACL и использование межсетевых экранов. Межсетевые экраны являются крайне эффективным способом защиты от DDoS-атаки. Межсетевой экран представляет собой программно-аппаратный комплекс, предназначенный для контроля и фильтрации, в соответствии с заданными правилами, проходящих через него пакетов.

3. Обратные DDoS-атаки – представляют собой перенаправление нелегитимного трафика на компьютер нарушителя, что позволяет его заблокировать и таким образом нейтрализовать атаку. Однако для этого необходимы значительные серверные мощности, которыми располагают крупные ведомственные сети. Кроме того, при наличии ошибок в программном коде операционных систем, системных служб или web-приложений данный тип защиты применить невозможно;

4. Устранение уязвимостей – данный тип защиты нацелен на устранение ошибок в тех или иных системах или службах (исправление эксплоитов, установка обновлений на операционную систему и т.п.). Очевидно, что этот метод защиты позволяет только выявить факт уже совершенного нарушителем воздействия и не является эффективным против так называемых flood-атак. Данное направление защиты, совместно с мониторингом сети, по значению коэффициента исправного действия, повышает ее защищенность на 30-40% за счет существенного сокращения времени обнаружения факта кибервоздействия и восстановления нормального функционирования сетевых элементов ИБС;

5. Построение распределенных и дублирующих систем – позволяет обслуживать пользователей, даже если некоторые узлы становятся недоступны из-за DDoS-атак. Рекомендуется строить распределенные системы, используя не только различное сетевое или серверное оборудование, но и физически разносить сервисы по разным Data-центрам. Распределенные системы позволяют справиться практически с любым типом атак при правильном архитектурном построении сети;

6. Мониторинг – установка системы мониторинга и оповещения, которая позволит вычислить DDoS-атаку по определенным критериям. Мониторинг напрямую не может защищать атакуемую систему, но позволяет вовремя среагировать и принять соответствующие меры.

СПИСОК ЛИТЕРАТУРЫ

1. https://aktualno.uz/ru/news/6381 – (дата обращения 01.10.2022 г.)
2. https://nova24.uz/money/gruppa-mezhdunarodnyh-hakerov-atakovala-uzbekskij-bank-i-prisvoila-sredstva/ – (дата обращения 01.10.2022 г.)
3. https://nova24.uz/incidents/v-tashkente-vzlomali-sistemu-davr-banka-i-pohitili-15-milliardov-sumov/ – (дата обращения 01.10.2022 г.)
4. https://www.gazeta.uz/ru/2021/06/30/kaspersky/ – (дата обращения 01.10.2022 г.)
5. Бекбаев, Г.А. Модель процесса «DDoS»-атаки на телекоммуникационную сеть железнодорожного транспорта / Г.А. Бекбаев, А.А. Привалов, Н.Б. Ачкасов, А.О. Кравцов // Изв. ПГУПС. – 2017. – Вып. 3 (52). – С. 420–426.
6. Бекбаев, Г.А. Подход к моделированию процесса DDoS-атаки на информационно-телекоммуникационную сеть железнодорожного транспорта / Г.А. Бекбаев, А.А. Привалов, О.А. Турдиев // Вестн. СамГУПС. – 2018. – Вып. 1. – С. 100–108.
7. Бекбаев Г.А. Методика оценки функциональной целостности сети оперативно-технологической связи на участке высокоскоростной железнодорожной магистрали «Ташкент-Самарканд» АО «УТЙ»: дис. … канд.технич.наук: 05.12.13 / Бекбаев Гамзатдин Алеуатдинович. – Спб., 2018. – 155 с.
8. Коцыняк М.А. Устойчивость информационно-телекоммуникационных сетей / М. А. Коцыняк, И. А. Кулешов, О. С. Лаута- СПб.:Изд-во Политехн. ун-та, 2013.– 92 с.

9. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с., ил.
10. Крылов Г. О. Компьютерные атаки с “Распределенным отказом в обслуживании” на вычислительные сети и механизмы защиты от них на основе структурно-статистического анализа входного потока данных / Г. О. Крылов, М. М. Тараскин, С. А. Чешуин // Безопасность информационных технологий, 2011. - №4. – С. 184-188.
11. Привалов А. А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ / А. А. Привалов. – СПб: ВМА, 2000. – 166 с.
12. Бекенова Я.А. Моделирование DDoS-атак и механизмов защиты от них/ Я. А. Бекенова, Н. Н. Шипилов, К. А. Борисенко, А. В. Шоров // Известия СПбГЭТУ «ЛЭТИ», 2015. - №3. – С. 32-39.
13. Конахович Г. Ф., Климчук В. П., Паук С. М., Потапов В. Г.Защита информации в телекоммуникационных системах. К.: «МК-Пресс», 2005. – 288 с., ил.
14. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А. А., Мещеряков Р. В. и др.; под.ред. А. П. Зайцева и А. А. Шелупанова. – М.: ООО «Издательство Машиностроение» 2009. – 508 с.
15. Вандич А.П. Методика оценки оперативности управления телекоммуникационной сетью ОАО «РЖД» в нестационарных условиях: дис. … канд. технич. наук: 05.12.13 / Вандич Алексей Павлович. – Спб.: ПГУПС, 2013. – 142 с.