УДК 004.056.53

Кирсанов И.Р., Студент
МГТУ им. Н.Э. Баумана
Россия, г. Москва
Полухина Д.Ю., Студент
МГТУ им. Н.Э. Баумана
Россия, г. Москва

ПРИМЕНЕНИЕ И РОЛЬ СИСТЕМЫ ЗАЩИТЫ SIEM В БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ.

Аннотация: *В статье рассматриваются основные угрозы в сфере информационной безопасности банка. Проблемы увеличения интенсивности обмена информацией и выявление критических инцидентов, которые обусловлены данным увеличением. Сформирована модель анализа информационных массивов. На основе аналитических результатов предложено внедрить SIEM систему.*

Ключевые слова: *SIEM, информационная безопасность, банк, критический инцидент, корпоративная сеть.*

Kirsanov I.R., Student
BMSTU
Russia, Moscow
Polukhina D.Yu., Student
BMSTU
Russia, Moscow

Application and role of the SIEM security system in banking.

Abstract: *The article discusses the main threats in the field of information security of the bank. Problems of increasing the intensity of information exchange and identifying critical incidents that are caused by this increase. The*

model of analysis of information arrays is formed. Based on the analytical results, it was proposed to implement the SIEM system.

Keywords: *SIEM, information security, bank, critical incident, corporate network.*

В современной российской рыночной экономике неотъемлемым условием успеха любого банка в получении максимальной прибыли, и сохранении целостности созданной им организационной структуры, является обеспечение информационной безопасности, применение систем безопасности, анализ потенциальных угроз.

Разумная реализация политики информационной безопасности в банках предполагает применение комплексного подхода, который заключается в применении технических, программных, правовых, организационных и социальных мер и средств защиты. Все перечисленные меры нацелены на обеспечение целостности и конфиденциальности информационных ресурсов, при сохранении их доступности для сотрудников организации в соответствии с их полномочиями.

Информационные системы разрабатываются для оказания установленных информационных услуг, в то же время если по каким-либо причинам получение таких услуг является невозможным, то данный факт способен нанести ущерб субъектам информационных отношений. В связи с этим доступность информации можно считать одним из важнейших элементов безопасности в целом и информационной в частности. Под доступностью понимается то, что информация должна быть в целостном виде, и находится в таком месте, что бы «заинтересованное» лицо могло получить в любое время необходимую информацию.

Так же можно выделить дополнительные элементы модели информационной безопасности [1. с.26], к ним относят: аутентичность и

аппелируемость.

Исходя из названия, к первому относят возможность персонификации человека, автора полученной или исходящей информации. Аппелируемость -это на прямую взаимосвязанное понятие с аутентичностью, и означает возможность доказательства того, что именно этот человек был автором предоставленной информации, и никто другой.

На современном этапе, концепция информационной защищённости рассматривает несколько классификаций рисков и угроз информации для банка. Более подробно и глубоко угрозы рассматриваются с точки зрения влияющей среды предприятия, и подразделяются на:

- Внешние угрозы;
- Внутренние угрозы.

Обратившись к статистическим данным [2. с.18] можно заметить, что если десятилетие назад на долю внутренних угроз информационной безопасности предприятия приходилось 82% угроз, 17% являлись внешними и только 1 % всех угроз был случайными, то сегодня ситуация изменилась, и теперь на долю внутренних угроз стало приходиться 70% (что на 12% меньше показателя 2006 года), в то время как количество внешних угроз увеличилось почти вдвое и их доля составила 29%, случайные угрозы по-прежнему занимают всего 1% в структуре угроз информационной безопасности предприятия (Рис. 2). На сегодняшний момент по данным аналитических центров наибольшую долю угроз безопасности информации хозяйствующих субъектов составляет деятельность киберпреступников (26%), 21% всех угроз составляют злоупотребления администраторов информационных сетей, 18% - Dos-атаки, 17% - безграмотность пользователей, 12% - нарушение правил обмена информацией на предприятии и 6% - деятельность спецслужб (Рис. 3).

Рис. 2 - Структура угроз информационной безопасности предприятия в 2002 и 2020 годах.

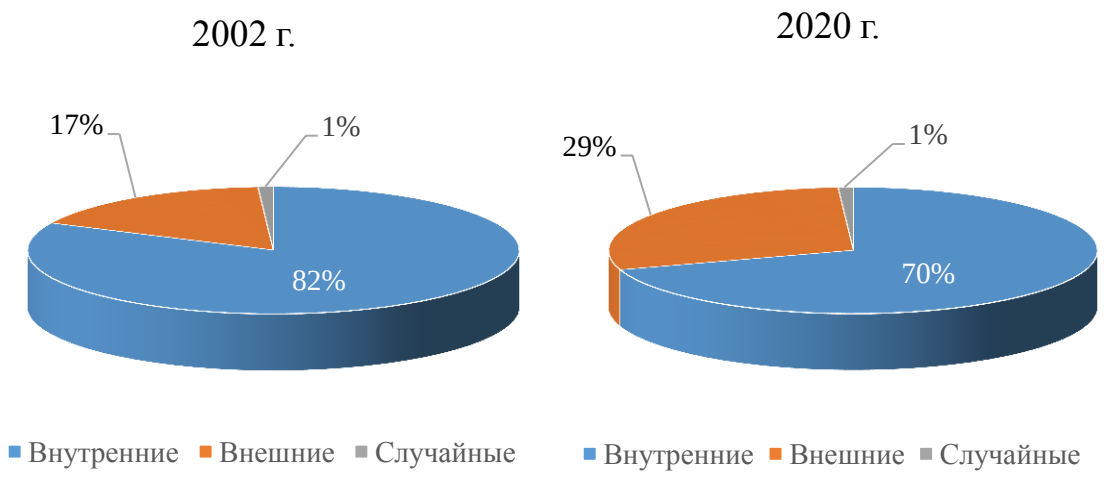
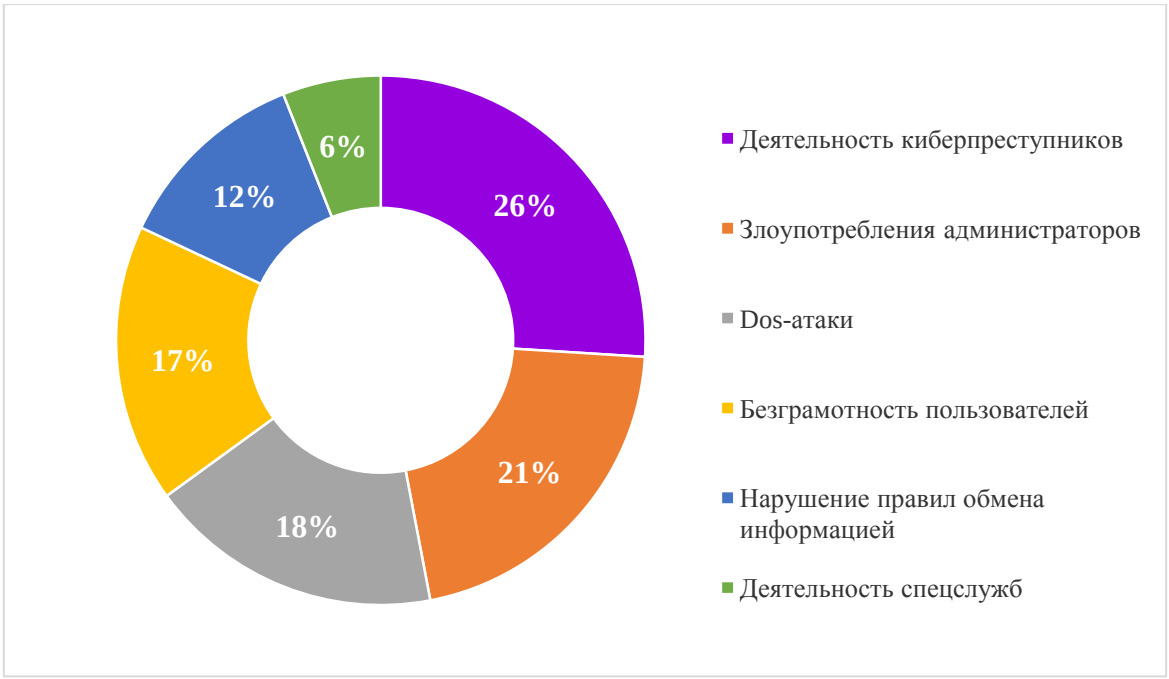


Рис. 3 - Инциденты информационной безопасности российских предприятий за 1-3 кварталы 2019 года.



Необнаруженные угрозы информационной безопасности организации становятся критическими инцидентами, которые могут оказать негативное влияние на деятельность всей компании в целом. Анализируя подробнее случаи в сфере информационной безопасности в основном крупных компаний, можно заметить, что большинство из них

связано со злоупотреблением администраторами своими полномочиями и передачей информации между сотрудниками информации внешним агентам по корпоративным сетям.

В связи с тем, что в банковской сфере повышенная интенсивность обмена информацией, которая обусловлена развитием и количеством бизнес-процессов, увеличивается опасность получения вредоносных файлов, бутфросов, фишингов. Интенсивность обработки и поступления информационных события в банке ежедневно может достигать до нескольких миллионов. Повышенная интенсивность всех событий не позволяет в ручном режиме провести анализ, так как требует большого количества временных затрат, и недопустимых под углом эффективности программного аппарата. Для банка решением данной проблемы может послужить внедрение SIEM систем.

SIEM система [3. с.126] представляет собой систему, которая появилась в результате объединения SEM-системы и SIM-системы. Главным отличием данных систем друг от друга является то, что система SEM предназначается для аналитики информации в режиме online, а SIM система, напротив, разработана для анализа исторических (накопленных) данных.

Основной задачей SIEM системы является анализ информации, поступающей из различных источников. Например, информация от систем антивирусной защиты, DLP, систем учета трафика, анализ уязвимости сетей и многих других. На основе данной информации SIEM проводит анализ и выявляет отклонения в системах при условиях стандартного функционирования, которые заданы основными критериями безопасности.

Внедрение SIEM системы в банке [4. с.38] не ограничивается функциями, описанными выше. Система может также быть использована для:

1. Любого анализа информации, которая поступает по различным

источникам.

2. Предоставления доказательств при внутренних расследованиях критических инцидентов информационной безопасности.
3. При аудите систем IT.
4. Непрерывность процесса работы посредством выявления сбоев информационных систем.
5. Структурирование телекоммуникационных обеспечивающих систем.

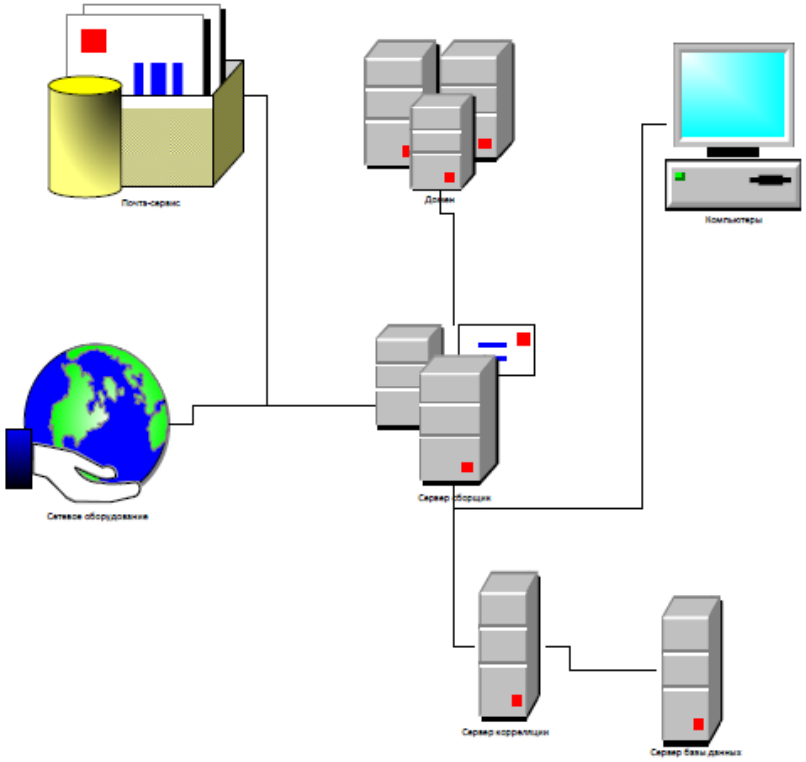
SIEM система решает такие задачи, как:

1. Анализ и разбор критических инцидентов;
2. Корреляция информационных событий;
3. Своевременное оповещение о критических инцидентах менеджмента банка.

Каждая SIEM система представлена основными компонентами, и дифференцирована на несколько уровней. Компоненты и системы (рис.4):

1. Агенты, которые запрограммированы на сбор информации из источников;
2. Сервер-коррелляторы;
3. Серверы сборщик, аккумулирующие информацию;
4. Сервер с базами данных.

Рис. 4 - основные компоненты SIEM системы.



SIEM система представлена несколькими уровнями:

1. Сбор логов и объединение данных из различных источников;
2. Приведение к единому формату событий, имеющих одинаковый логический смысл.
3. Коррелирование событий между собой.
4. Хранение лог-файлов.
5. Формирование визуального отчета для менеджеров.

Таким образом, рассматриваемая система в значительной степени упрощает работу для head-руководителей банка. Каждый критический инцидент сохраняется и регистрируется, что означает выявление ответственного лица за обработку критического инцидента. На основе исторических данных руководитель может сделать выводы об эффективности работы вовлеченного ответственного подразделения по защите и недопущению утечки информации. Благодаря данной системе представляется возможным составить автоматизированные и обновляемые

отчеты с визуальными составляющими.

Актуальность использования SIEM системы банками заключается в следующем:

1. Банк должен регулярно (ежеквартально, ежегодно) проводить аудит на предмет соответствия требований информационной безопасности банка.
2. В банке очень большой поток конфиденциальной информации, утечка которой может нанести не только репутационный вред банку, но и повлечь за собой невосполнимые финансовые потери.
3. Банк как финансовая организация со стабильно высокой прибылью имеет финансовую возможность приобрести и внедрить рассматриваемую систему.
4. Требование о наличие данной системы в банке установлено документально. Например, ISO 27001, SOX и другие.

Стремительное развитие рынка информационных услуг, модернизация и увеличение возможностей SIEM систем увеличивает как банковский спрос на продукт, так и иных организаций. С 2010 по 2019, экспертами были озвучены данные о том, что объем рынка информационных систем и технологий увеличился с 10 миллионов долларов дл 24 миллионов долларов. Кроме того, эксперты прогнозируют значительный рост покупки таких систем, так как с каждым годом защищенность информационного поля снижается.

Список используемой литературы:

1. Бабаш А. В., Ларин Д. А. История защиты информации в зарубежных странах: Учебное пособие. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2018.

2. Балановская А. В. Анализ современного состояния угроз информационной безопасности предприятий. // Информационная безопасность регионов. -2017. - № 3 (20).

3. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие. - 2-е изд. - М.: Форум: НИЦ ИНФРА-М, 2019.

4. Лазуткин А.Н. Аудит информационной безопасности на промышленном предприятии // Новая наука: стратегии и векторы развития. -2018. - № 5-2.