Международный союз электросвязи

МСЭ-Т X.1157

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2015)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасные приложения и услуги –
Протоколы безопасности

Технические возможности по обнаружению мошенничества и реагированию в случае услуг с высокими требованиями к уровню гарантии

Рекомендация МСЭ-Т X.1157

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	**X.1150–X.1159**
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
Рекомендации, связанные с PKI	X.1340–X.1349
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1157

Технические возможности по обнаружению мошенничества и реагированию в случае услуг с высокими требованиями к уровню гарантии

Резюме

В Рекомендации МСЭ-Т X.1157 представлены возможности, требуемые для обеспечения услуги обнаружения мошенничества и реагирования в рамках прикладных услуг информационно-коммуникационных технологий (ИКТ), чувствительных к безопасности. Услуги обнаружения мошенничества и реагирования помогают в обнаружении и анализе случаев мошенничества и противодействии им для разных пользователей, счетов, продуктов, процессов и каналов. В ней отслеживаются и анализируются активность и поведение пользователей на прикладном уровне (а не на уровне системы, базы данных или сети), а также отмечается, что происходит в рамках аккаунтов (учетных записей) и между различными аккаунтами с использованием любых каналов, доступных для пользователя. Кроме того, в ней анализируется поведение различных пользователей, аккаунтов или других структур путем отслеживания аномального поведения, случаев коррупции или неправомерного использования. Наиболее часто это применяется в вертикальных структурах, управляющих денежными средствами клиентов, таких как электронные финансы, удаленный доступ к корпоративной сети и т. д., но не менее часто используется для обнаружения случаев внутреннего мошенничества и других видов несанкционированной деятельности.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1157	17.09.2015 г.	17-я	11.1002/1000/12353

Ключевые слова

Система обнаружения случаев мошенничества, меры противодействия мошенничеству.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://handle.itu.int/, после которого следует уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу http://www.itu.int/ITU-T/ipr/.

Содержание

Рекомендация МСЭ-Т X.1157

Технические возможности по обнаружению мошенничества и реагированию в случае услуг с высокими требованиями к уровню гарантии

1 Сфера применения

В настоящей Рекомендации приведены руководящие указания по техническим возможностям систем противодействия мошенничеству в случае услуг с высокими требованиями к уровню гарантии. Целью данной Рекомендации является представление системы, способной обнаруживать мошеннические действия. Настоящая Рекомендация может применяться во многих коммерческих и производственных сферах деятельности, использующих прикладные услуги информационно-коммуникационных технологий (ИКТ), чувствительных к безопасности, путем внедрения системы обнаружения случаев мошенничества и реагирования на них. Кроме того, настоящая Рекомендация может использоваться для противодействия мошенничеству внутри организации, а также мошенническим действиям, производимым извне при помощи удаленного доступа или при предоставлении коммерческих услуг. В настоящей Рекомендации рассматриваются следующие области деятельности:

– возможности услуг по обнаружению случаев мошенничества и реагированию на них;

– функционирование и составные компоненты системы по обнаружению случаев мошенничества и реагированию на них; и

– соображения, касающиеся услуг защиты от происшествий и реагирования на них.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определяемые в других документах

В настоящей Рекомендации используются следующие термины, определяемые в других документах:

3.1.1 уровень гарантии (assurance level) [b-ITU-T X.1252]: Уровень доверия в отношении связи между объектом и представленной информацией идентичности.

3.1.2 аутентификация объекта ((entity) authentication) [b-ITU-T X.1252]: процесс, используемый для достижения достаточной меры доверия в отношении связи между объектом и представленной информацией идентичности.

ПРИМЕЧАНИЕ. – Использование термина "аутентификация" в контексте управления определением идентичности (IdM) означает аутентификацию объекта.

3.1.3 гарантия обеспечения аутентификации (authentication assurance) [b-ITU-T X.1252]: Степень доверия, достигаемого в процессе аутентификации, в отношении того, что партнер по связи является тем самым объектом, которым он себя заявляет или которым он должен быть согласно ожиданиям.

ПРИМЕЧАНИЕ. – Доверие основано на степени доверия в отношении связи между взаимодействующим объектом и представленной информацией идентичности.

3.1.4 конечный пользователь (end user) [b-ITU-T X.1141]: Физическое лицо, использующее ресурсы для решения прикладных задач.

3.1.5 идентичность (identity) [b-ITU-T X.1252]: Представление того или иного объекта в виде одного или нескольких атрибутов, которые позволяют однозначно и в достаточной мере распознать объекты в том или ином контексте. В целях управления определением идентичности (IdM) термин "идентичность" толкуется как контекстуальная идентичность (подмножество атрибутов), то есть разнообразие атрибутов ограничивается рамками с определенными граничными условиями (контекстом), в которых объект существует и взаимодействует с другими объектами.

ПРИМЕЧАНИЕ. – Каждый объект представлен одной целостной идентичностью, которая включает все возможные элементы информации, характеризующие такой объект (атрибуты). Вместе с тем такая целостная идентичность является теоретическим понятием и не может быть описана и практически использована, поскольку количество всех возможных атрибутов бесконечно.

3.1.6 гарантия определения идентичности (identity assurance) [b-ITU-T X.1252]: Степень доверия в процессе валидации и верификации, используемом для установления идентичности объекта, которому были предоставлены полномочия, и степень доверия в отношении того, что объект, использующий полномочия, является данным объектом или объектом, которому полномочия были предоставлены или переданы.

3.1.7 проверка подлинности идентичности (identity proofing) [b-ITU-T X.1252]: Процесс, в ходе которого выполняется валидация и верификация объема информации, достаточного для подтверждения заявленной идентичности объекта.

3.1.8 верификация идентичности (identity verification) [b-ITU-T X.1252]: Процесс подтверждения подлинности заявленной идентичности путем сравнения предложенных заявлений идентичности с ранее проверенной информацией.

3.1.9 поставщик услуг (service provider) [b-ITU-T X.1141]: Роль, выполняемая объектом системы, согласно которой он предоставляет услуги клиентам или другим объектам системы.

3.2 Термины, определяемые в настоящей Рекомендации

В настоящей Рекомендации используются следующие термины.

3.2.1 система обнаружения случаев мошенничества (fraud detection system): Программное обеспечение в качестве прикладной программы, которое позволяет проводить наблюдения, обнаруживать случаи мошенничества и противодействовать таким случаям или другим злоупотреблениям в отношении пользователей (например, клиентов), счетов, каналов, продуктов и прочих объектов (например, интерактивных терминалов).

ПРИМЕЧАНИЕ. – При внедрении системы обнаружения случаев мошенничества корпоративные приложения могут объединяться с подсистемой обнаружения случаев мошенничества, производящей оценку рисков совершения мошеннических действий при проведении пользователем транзакции от навигации и доступа к приложениям до любых иных действий, таких как изменение адреса, осуществление платежей или извлечение конфиденциальной информации.

3.2.2 противодействие мошенничеству (fraud management): Полный комплекс мероприятий, включающих системы раннего предупреждения, признаки и модели различных видов мошеннических действий, профили пользователей и их действия, реагирование на инциденты и т. д. и призванных уменьшить риски для безопасности при помощи систем обнаружения случаев мошенничества.

ПРИМЕЧАНИЕ. – Разработка систем противодействия мошенничеству необходима ввиду наличия ряда проблем, включая огромный объем обрабатываемых данных; необходимость быстрого и точного обнаружения мошеннических действий без создания при этом помех хозяйственной деятельности;

регулярное появление новых видов мошенничества в обход существующих методов противодействия; а также риск генерации ложных тревог.

3.2.3 приложение информационно-коммуникационных технологий (ИКТ), чувствительное к безопасности (security sensitive information and communication technology (ICT) application): Приложение, требующее чрезвычайно высокого уровня гарантии безопасности для защиты информационных активов частных лиц, организаций и/или предприятий, владеющих конфиденциальной информацией.

ПРИМЕЧАНИЕ. – Взлом и контроль злоумышленником приложений ИКТ, чувствительных к безопасности, может привести к раскрытию конфиденциальной, то есть личной или финансовой, информации, что повлечет за собой массированное вредоносное воздействие на пользователей, организации, инфраструктуру и службы электросвязи, к которым относятся приложения для электронных платежей, услуги электронного здравоохранения и удаленный доступ предприятий.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

API	Application Programming Interface	Интерфейс прикладного программирования
ATM	Automated Teller Machine	Автоматизированный кассовый аппарат
DLP	Data Loss Prevention	Предотвращение потери данных
DNS	Domain Name System	Система доменных имен
DSL	Digital Subscriber Line	Цифровая абонентская линия
GSM	Global System for Mobile Communications	Глобальная система подвижной связи
HTTP	HyperText Transfer Protocol	Протокол передачи гипертекста
ICT	Information and Communication Technology	Информационно-коммуникационные технологии
ID	Identity	Идентичность
IP	Internet Protocol	Интернет-протокол
IPS	Intrusion Prevention System	Система предотвращения проникновений
ISP	Internet Service Provider	Поставщик интернет-услуг
IT	Information Technology	Информационные технологии
MITM	Man-in-the-Middle	Человек посередине
NAC	Network Access Control	Контроль доступа к сети
OS	Operating System	Операционная система
PC	Personal Computer	Персональный компьютер
PIN	Personal Identity Number	Личный идентификационный номер
SMS	Short Message Service	Служба коротких сообщений
SP	Service Provider	Поставщик услуг
SQL	Structured Query Language	Язык структурированных запросов
SSL	Secure Socket Layer	Уровень безопасных соединений
TAN	Transaction Authentication Number	Номер транзакции
WiMAX	Worldwide Interoperability for Microwave Access	Всемирная функциональная совместимость для микроволнового доступа

5 Соглашения по терминологии

Слова "требуется, чтобы" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии этой Рекомендации.

Слова "рекомендуется, чтобы" означают требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, для заявления о соответствии это требование не является обязательным.

Слово "запрещается" означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии данной Рекомендации.

Слова "может быть дополнительно" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Этот термин не означает, что вариант реализации поставщика должен обеспечивать выполнение данной функции и что функция может быть активирована по желанию оператора сети/поставщика услуг. Это означает лишь, что поставщик может дополнительно предоставить эту функцию и по-прежнему заявлять о соответствии этой Рекомендации.

6 Общие аспекты обнаружения случаев мошенничества и реагирования на них

6.1 Формулировки проблемы

В сфере прикладных услуг, основанных на электросвязи, целенаправленным хакерским атакам с использованием вредоносных программных средств подвергаются многие типы компаний и отраслей вертикальных услуг (например, электронная доставка, электронная больница и другие виды электронных услуг). Интенсивность этих атак постоянно растет и вызывает серьезное беспокойство. Как правило, они производятся с использованием целенаправленных фишинговых сообщений электронной почты, а также объектов, содержащих вредоносную программу, например рекламных объявлений, по которым кликают неопытные пользователи. С использованием подобных методов было заражено большое количество организаций.

Многие организации, ведущие разнообразную коммерческую и предпринимательскую деятельность, подвергаются значительным рискам, связанным с потерей данных, несанкционированным доступом к учетным записям и проведением транзакций от внешних и внутренних источников. Целенаправленные вредоносные программы зачастую способны обходить существующие технологии защиты, и произошедший в результате несанкционированный доступ к данным оказывается незамеченным в течение продолжительного времени, пока не обнаружится значительная утечка данных. Признаки вредоносных действий, как правило, оказываются "спрятанными на видном месте" и не могут быть обнаружены в связи с отсутствием возможности мониторинга и неспособности отличить пример аномальной работы приложения или несанкционированного доступа к данным от примеров нормальной работы. К примеру, клиенты банка могут не подозревать о совершенных мошеннических действиях до тех пор, пока не увидят счет, который не был подтвержден в отчете о кредитных операциях, или пока к ним не обратится коллектор с требованием об оплате задолженности.

Хакерские атаки, направленные против клиентов финансовых учреждений и сотрудников компаний, наносят серьезный репутационный и финансовый ущерб своим жертвам. Эти атаки все активнее используются для взлома учетных записей клиентов и организаций и кражи конфиденциальной информации или денежных средств. Следовательно, пока коммерческая деятельность предприятия не будет должным образом организована в целях эффективного

обнаружения мошенничества, серьезные предупреждения об опасности и сигналы тревоги могут игнорироваться. Наконец хакерские атаки могут применяться для завладения номерами банковских счетов пользователей, а также для совершения мошенничества или кражи серверных ресурсов.

6.2 Роль противодействия мошенничеству

Система противодействия мошенническим действиям может применяться в трех типичных случаях мошенничества:

- обнаружение захвата номеров банковских счетов, происходящего, как правило, в результате кражи регистрационных данных пользователя или внедрения вредоносного программного обеспечения (хакерских программ). Хакерские программы могут проникнуть в компьютерную систему предприятия не только через инфицированные документы, прикрепленные к сообщениям электронной почты, но и при простом посещении зараженного веб-сайта;
- обнаружение мошеннических действий в отношении новой учетной записи, происходящих в результате кражи регистрационных данных пользователя или внедрения вредоносного программного обеспечения (хакерских программ);
- обнаружение использования украденной (или чужой) учетной записи, например украденной кредитной карты при совершении покупок либо имитации поведения обычного пользователя.

Система противодействия мошенничеству чаще всего используется для одного или нескольких случаев мошеннических действий, таких как овладение номером банковского счета, для обнаружения внутреннего мошенничества, обнаружения мошенничества с использованием платежных карт в реальном времени и блокировки транзакций, а также в качестве системы пресечения особых видов мошенничества или злоупотреблений на предприятиях. В каждом из приведенных сценариев предприятие, производящее обработку транзакции, обязано проверять легитимность лица, выполняющего данную транзакцию.

6.3 Основные функции системы противодействия мошенничеству

Если вести речь о полномасштабном противодействии мошенническим действиям с персональными данными, система обнаружения случаев мошенничества должна быть способна выполнять три функции, позволяющие решать данную задачу, – мониторинг, обнаружение и реагирование на инциденты. Эти функции включают меры, принимаемые для выявления подозрительных действий, в первую очередь на основании информации о различных событиях; меры по обнаружению мошенничества на ранней стадии затрагиваемого процесса; а также меры, принимаемые для распознавания мошенничества при обнаружении тех или иных подозрительных действий.

Мониторинг – система обнаружения случаев мошенничества может отследить мошеннические действия путем поиска аномальных отклонений в поведении и действиях пользователей на прикладном уровне, а также на уровне системы, базы данных или сети. Кроме того, эта система наблюдает за тем, что происходит в рамках отдельных счетов и между различными счетами, используя любые каналы, доступные пользователям. Она также отслеживает и анализирует поведение пользователей или аккаунтов и связанные с этим транзакции и выявляет аномальное поведение, используя правила или статистические модели. Кроме того, система может (в оптимальным варианте) использовать непрерывно обновляемые профили и учетные записи пользователей, а также одноранговых групп, сравнивая транзакции и выявляя среди них подозрительные. В частности, для тщательного отслеживания внутренних мошеннических действий необходим мониторинг привилегированных

пользователей информационных технологий (IT), которые могут напрямую вносить изменения в файлы и данные, в отличие от тех, которые используют обычные пользовательские приложения.

Обнаружение – система обнаружения случаев мошенничества способна обрабатывать, разбивать на части и анализировать большие объемы данных с использованием сложных взаимосвязей и сортировки по правилам, определяемым коммерческими организациями, в целях предотвращения мошенничества. Она может использоваться для обнаружения мошенничества со стороны как внутренних злоумышленников (например, сотрудников), так и внешних (например, клиентов или партнеров по бизнесу). Для поддержки функций обнаружения мошенничества система может и должна классифицировать различные объекты, такие как пользователи, учетные записи, домашние хозяйства, персональные компьютеры (ПК), мобильные телефоны и интерактивные терминалы, в целях выявления аномального поведения данного объекта при выполнении транзакции. При обнаружении мошенничества применяется политика на основе правил, базирующаяся на человеческих суждениях и знаниях, а также на математических моделях прогнозирования, помогающих оценить вероятность мошеннических действий для той или иной транзакции.

Реагирование (на случаи мошенничества) – после обнаружения подозрительной активности система противодействия мошенничеству должна реагировать на подозрительные действия и принимать различные меры предосторожности, такие как блокировка счетной записи или обмен информацией. Разнообразные дополнительные технологии мониторинга и обнаружения могут помочь организациям более эффективно обнаруживать подозрительные действия пользователей, распознавать схемы несанкционированного доступа к ресурсам или мошеннических операций с учетными записями, а также проводить расследования инцидентов и принимать по ним надлежащие меры, в частности оповещение в реальном времени, урегулирование инцидентов, блокировку учетной записи либо прерывание транзакции. Таким образом, организациям необходимо определить, какие комбинации технологий мониторинга и анализа в наибольшей степени соответствуют их уровням рисков. Кроме того, необходимо определиться с их возможностями по реализации и поддержке технологий обеспечения безопасности.

7 Архитектура системы обнаружения случаев мошенничества и реагирования на них

7.1 Принцип действия и компоненты

Приложения ИКТ могут быть объединены с компонентами обнаружения случаев мошенничества, тем самым обеспечивая основные функциональные возможности по снижению рисков мошенничества в отношении транзакций пользователей, имеющих доступ к любому из видов деятельности. Принцип действия системы обнаружения мошенничества не должен быть прозрачным ни для хакеров, ни для пользователей, с тем чтобы хакеры не смогли узнать правила работы системы и чтобы соответственно не доставлять неудобств законопослушным пользователям. Подозрительные транзакции пользователей подвергаются повторной проверке в реальном времени. Тем самым система обнаружения мошенничества производит оценку их легитимности. Транзакция может быть приостановлена до момента, когда система обнаружения мошенничества сможет произвести проверку ее легитимности.

Система обнаружения мошенничества состоит из нескольких компонентов, осуществляющих обработку, хранение и передачу данных в целях обнаружения аномальных действий. Принцип действия системы обнаружения мошенничества заключается в обработке данных, которыми обмениваются компоненты системы. Операции и компоненты системы обнаружения

мошенничества подробно показаны на рисунке 1. В идеальном варианте система обнаружения мошенничества запускает мониторинг всего сеанса работы с момента первоначального входа пользователя в систему. Соответственно система обнаружения мошенничества выполняет операции по противодействию мошенничеству, то есть от возможностей мониторинга до способности к мерам реагирования, как показано ниже.

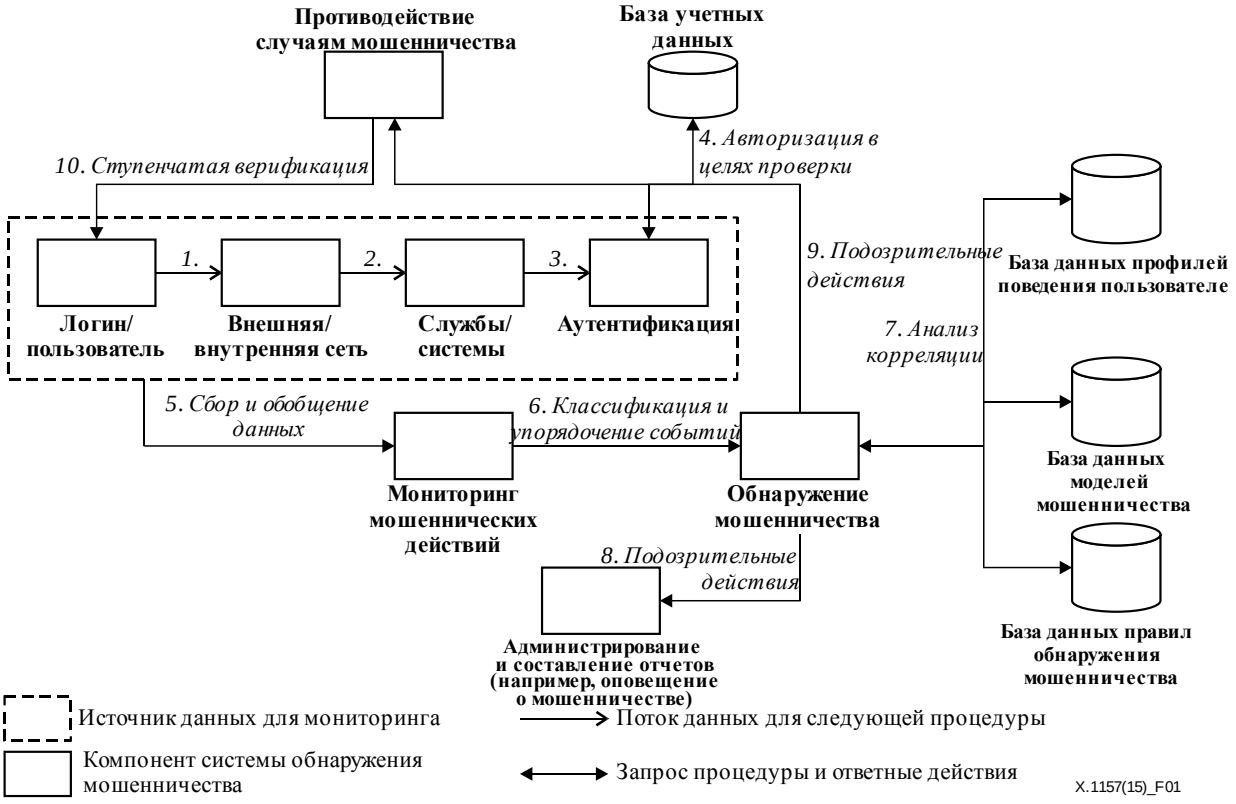

Рисунок 1 – Операции и компоненты системы обнаружения мошенничества

Процедуры ввода логина и пароля, аутентификации и авторизации в целях проверки (потоки данных 1, 2, 3 и 4)

В обычной ситуации анализу подвергается процедура первого входа в систему. Затем учетные данные, собранные в процессе входа в систему, сравниваются с информацией, находящейся в базе учетных данных пользователей (имена пользователей и пароли), IP-адресом, базой данных профилей поведения пользователей и т. д. По результатам этой процедуры определяется количественный показатель риска. Авторизация в целях проверки выполняется согласно правилам аутентификации, определенным в базе учетных данных, конфигурация которой, как правило, осуществляется организацией. База может расширяться путем добавления новых правил.

Процедуры мониторинга, обнаружения случаев мошенничества и противодействия им (потоки данных 5, 6, 7, 9 и 10)

После авторизации пользователя система обнаружения случаев мошенничества производит сбор информации из различных источников (то есть сетей, служб систем и на основе аутентификации). Система обнаружения мошенничества анализирует данные, полученные от компонента, отвечающего за мониторинг случаев мошенничества. Например, если в процессе аутентификации выявлены те или иные сомнительные действия, система обнаружения случаев мошенничества направляет подозрительные данные компоненту,

отвечающему за обнаружение этих инцидентов. Затем компонент, отвечающий за обнаружение, посылает запрос для анализа корреляции в базах данных, содержащих информацию о мошеннических действиях (то есть данные по профилям поведения пользователей, модели мошеннических действий и правила обнаружения мошенничества). Случаям мошенничества присваиваются приоритеты на основании уровней рисков, полученных от компонента, отвечающего за обнаружение таких случаев. Таким образом, формируется полная картина рисков, связанных с взаимодействиями, имеющими высокие количественные показатели риска. В случае выявления высокого уровня риска мошенничества компонент, отвечающий за противодействие случаям мошенничества, запрашивает более серьезную проверку для пользователя, вошедшего в систему. Решения по случаям мошенничества могут и должны отправляться обратно в базы данных. Таким образом формируется самообучающаяся замкнутая система, позволяющая улучшить эксплуатационные характеристики системы в будущем.

Операции администрирования и подготовки отчетов (поток данных 8)

Необходимо, чтобы организация могла использовать также компонент, отвечающий за администрирование и подготовку отчетов. Это позволит более подробно изучить систему обнаружения случаев мошенничества и более эффективно ею управлять. Данный компонент дает возможность пользователям системы беспрепятственно проводить анализ и составлять отчеты по функциональным характеристикам системы, выявлять противоречия в оценке или доступе, определять элементы системы, которые можно усовершенствовать, а также отслеживать действия пользователей и эксплуатационные показатели системы. Кроме того, средства подготовки отчетов обеспечивают наглядное представление подробной информации о характеристиках системы для руководства компании и специалистов, занимающихся анализом случаев мошенничества.

7.2 Соображения, касающиеся архитектуры

При внедрении системы обнаружения мошеннических действий для ИКТ-приложений применяются три вида архитектуры: модули обнаружения случаев мошенничества, встроенные в сервер приложений (например, веб-сервер), прослушивание и/или мониторинг онлайн-приложения и программные интерфейсы для унаследованных приложений. Наиболее важными факторами, определяющими эффективность приложений, являются правила и процессы, отражающие деятельность организации.

Модуль обнаружения случаев мошенничества, размещенный внутри сервера приложений

Правила, установленные организацией, применяются посредством фильтра ко всем запросам по протоколу передачи гипертекста (HTTP) (например, вход в систему или платеж), перед тем как транзакция обращается к приложению. Транзакции могут быть остановлены или перенаправлены на процедуру верификации транзакции в реальном времени путем выполнения правил обнаружения мошеннических действий для данного модуля. Некоторые поставщики предоставляют плагины для серверов приложений, встроенные непосредственно в предварительный процессор.

Прослушивание и/или мониторинг приложения ИКТ (режим прослушивания)

В этом режиме приложение прослушивает или анализирует входящие файлы или сетевой трафик HTTP (например, процесс входа в систему) либо считывает данные, используя плагины для серверов приложений, установленные на каждом сервере. Данные считываются в режиме реального времени (метод анализатора сетевых пакетов) или в режиме, близком к реальному времени (метод прослушивания серверов приложений), а затем передаются

другому приложению для борьбы с мошенничеством либо преобразуются в формат, при котором могут применяться правила обнаружения мошеннических действий. В последнем случае подозрительные транзакции приостанавливаются, а затем передаются на рассмотрение специалисту-аналитику по вопросам мошенничества. Специально настроенные интерфейсы прикладного программирования (API) могут объединяться таким образом, чтобы транзакции перенаправлялись на процедуру проверки типа запрос/ответ.

Программные интерфейсы для унаследованных приложений (режим встраивания в процесс)

В данном случае для проведения всех транзакций через систему обнаружения мошеннических действий (до обработки транзакции) используются интерфейсы API. Поток транзакций контролируется, и в случае обнаружении подозрительной транзакции пользователь может быть подвергнут проверке в реальном времени. Изменения бизнес-правил требуют внесения изменений в базовое приложение. Работа интерфейсов API основана главным образом на веб-услугах. Кроме того, интерфейсы API усложняют переход от одной конкретной системы, определяемой поставщиком, к другой.

Как правило, применение интерфейсов API для обнаружения случаев мошенничества позволяет предприятиям/организациям непосредственно контролировать поток транзакций, однако при этом необходима значительная работа по интеграции. Кроме того, при изменении базового приложения интерфейсы должны постоянно обновляться. Для серверов приложений, не требующих вмешательства в транзакции пользователей в реальном времени, предпочтителен второй метод, наиболее простой с точки зрения отказа или замены.

8 Технические возможности обнаружения случаев мошенничества и реагирования на них

8.1 Возможности мониторинга

Возможность мониторинга устанавливает связь пользователей и данных, необходимую для обнаружения атак и несанкционированного доступа на раннем этапе, а также обеспечивает возможность мониторинга доступа к данным и действий пользователей. Кроме того, общим требованием для составления отчетов о соответствии является мониторинг привилегированных пользователей и доступа к конфиденциальным данным.

Для системы обнаружения мошеннических действий необходима функция управления конфиденциальной информацией и администрирования событий, позволяющая осуществлять широкомасштабный мониторинг активности пользователей и доступ к ресурсам в сетях, системах, базах данных и приложениях. Система обнаружения мошеннических действий нуждается также в дополнении данных о событиях контекстной информацией о пользователях, активах, угрозах и уязвимостях в целях повышения эффективности мониторинга обеспечения безопасности для обнаружения несанкционированного доступа. Кроме того, эта система требует выборочного дополнения функции общего мониторинга безопасности такими возможностями, как мониторинг угроз повышенной сложности, основанный на оценке риска, а также внедрение и эффективная эксплуатация системы обнаружения мошеннических действий и реагирования на них.

Система обнаружения мошенничества собирает также данные о событиях почти в реальном времени при помощи способа, позволяющего немедленно проводить анализ. Возможность мониторинга в реальном времени имеет большое значение с точки зрения нейтрализации угроз для отслеживания и анализа развития атаки по компонентам и системам, а также для мониторинга в целях отслеживания и анализа активности пользователя в приложениях либо

для отслеживания и анализа серии связанных транзакций или событий доступа к данным. И наконец, возможность мониторинга в реальном времени должна поддерживать пакетный сбор данных в тех случаях, когда сбор данных в реальном времени не является целесообразным или необходимым.

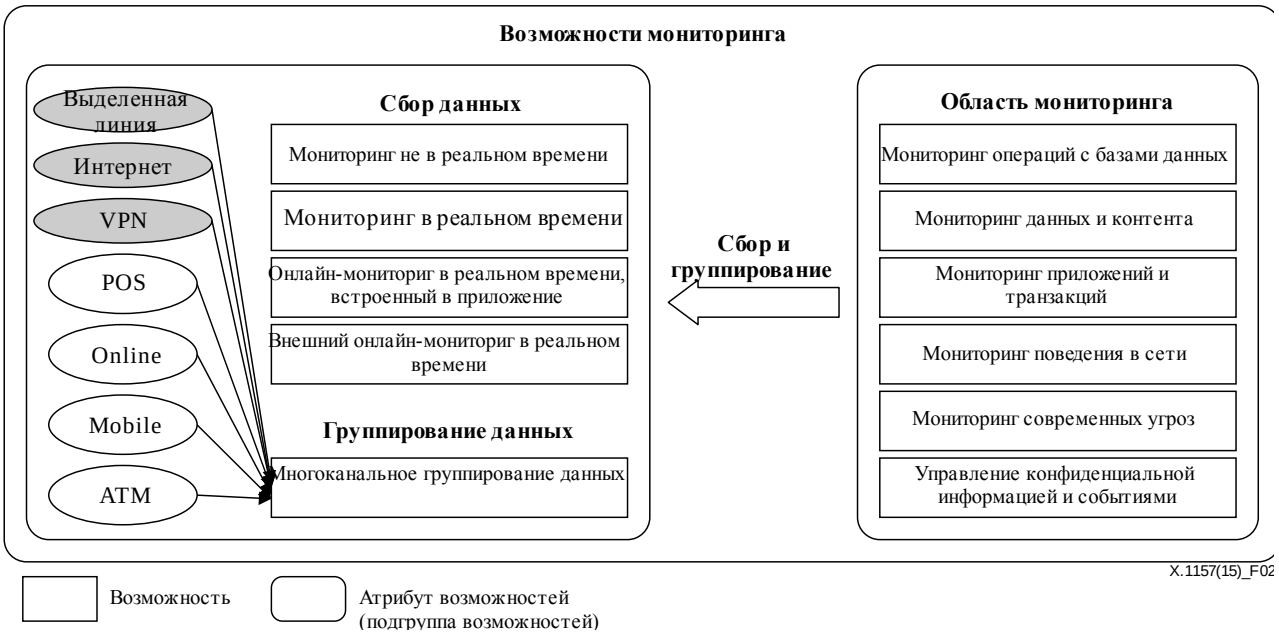

Рисунок 2 – Система обнаружения мошенничества. Функции мониторинга

8.1.1 Группирование и сбор данных

Операции по группированию и сбору данных поддерживаются для самых разнообразных источников зарегистрированных данных, включая журналы сетевых устройств и приборов системы безопасности, серверов, баз данных и приложений, выходные данные приложений, связанных с безопасностью, таких как мониторы оценки уязвимости и действий с базами данных, а также выходные данные соответствующих технологий управления идентичностью и доступом, в числе которых системы каталогов, регистрации пользователей и управления доступом на предприятиях.

Мониторинг не в реальном времени

Мониторинг не в реальном времени требует ручного или автоматического просмотра файлов журнала. Данная функция может предоставлять варианты быстрого развертывания для анализа, проводимого после транзакции, с более длительными периодами проверки и отменять возможность приостановки транзакций в точке завершения. Эта функция должна поддерживать пакетный сбор данных в тех случаях, когда сбор данных в реальном времени не является целесообразным или необходимым.

Мониторинг в реальном времени

Мониторинг в реальном времени отслеживает все транзакции (например, HTTP) в реальном времени с использованием фильтра веб-сервера. Данная функция может осуществлять контроль без применения дополнительного аппаратного обеспечения с использованием фильтра веб-сервера с низким уровнем воздействия. Для просмотра любых данных о транзакциях в реальном времени нет необходимости вносить какие бы то ни было изменения в приложения.

Функция онлайн-мониторинга в реальном времени, встроенная в приложение

Функция онлайн-мониторинга в реальном времени, встроенная в приложение, отслеживает все веб-транзакции, использующие протокол HTTP, при помощи интеграции в приложение. Установка и поддержка данной функции могут оказаться затратными с точки зрения стоимости и времени, поскольку для мониторинга транзакции в определенных точках потребуется внесение существенных изменений в приложения.

Внешний онлайн-мониторинг в реальном времени

Функция внешнего онлайн-мониторинга в реальном времени отслеживает все веб-транзакции, использующие протокол HTTP при помощи внешнего фильтра приложения. Данная функция не влияет на приложение при использовании методов анализатора сетевых пакетов и веб-фильтра, однако внешний фильтр встроен в приложение, а это может поставить под угрозу надежность приложения. Для просмотра любых данных о транзакциях в реальном времени нет необходимости вносить какие бы то ни было изменения в приложениях.

Многоканальное группирование данных

Многоканальное группирование данных означает, что данные о транзакциях, полученные из других каналов, могут быть полностью включены в процессы мониторинга и обнаружения случаев мошенничества. Кроме того, многоканальное группирование данных позволяет отслеживать подозрительное поведение пользователя или аккаунта, и в то же время обладает такими преимуществами, как просмотр каналов и продуктов, корреляция оповещений и действий для каждого пользователя, аккаунта или объекта. Многоканальное группирование данных позволяет анализировать взаимосвязи между внутренними и/или внешними объектами и их атрибутами (в числе которых пользователи, аккаунты, атрибуты аккаунтов, компьютеры и атрибуты компьютеров) в целях обнаружения аномальных действий или злоупотреблений.

8.1.2 Контролируемый источник данных

Система обнаружения случаев мошенничества способна выявлять злонамеренные действия в непрерывном потоке отдельных событий, которые, как правило, связаны с авторизованным пользователем и генерируются несколькими источниками в сетях, системах и приложениях. Возможности мониторинга включают интеграцию с несколькими источниками, позволяющую получить информацию о подозрительных событиях и нештатных ситуациях.

Мониторинг операций с базами данных

Мониторинг операций с базами данных помогает поддерживать разделение обязанностей для пользователей, имеющих привилегированный доступ к базе данных, путем мониторинга действий администраторов. Эта функция также повышает уровень безопасности базы данных за счет обнаружения нарушений правил и аномальных действий. Группирование событий, корреляция и формирование отчетов, связанных с базами данных, позволяют проводить аудит базы данных, не требующий наличия встроенной функции аудита.

Данная функция мониторинга поддерживает возможность поиска изменений в структуре и содержимом базы данных, а также доступ к данным для привилегированных пользователей при помощи локальной или удаленной авторизации. Поскольку данная функция работает на уровне базы данных и файлов, в ней отсутствует контекст какого-либо доступа к информации и навигации, которые не относятся к базе данных или связанным с ней файлам. Сетевые компоненты мониторинга (встроенные или внешние) могут использоваться для отслеживания SQL-запросов (язык структурированных запросов) и административного сетевого доступа.

Мониторинг данных и контента

Возможности мониторинга данных и контента часто используются для ограничения утечек информации, такой как номера кредитных карт, информация для идентификации личности и объекта интеллектуальной собственности на основе документов или базы данных, вместе с функцией поддержки мониторинга контента, фильтрации и предотвращения потери данных (DLP). Задачей рассматриваемой функции является предоставление организации возможности отслеживания собственного внутреннего контента в целях выявления подозрительных действий. Мониторинг и фильтрация контента используются для защиты контента в процессе его передачи (при помощи сетевого мониторинга или фильтрации), в дежурном режиме (через сканирование хранилища) и в процессе использования (при помощи агентов оконечной точки). Большинство функций включают также возможности сканирования сохраненного контента в сети на наличие нарушений политики (например, номер кредитной карты или несанкционированный сервер), поиска нарушений корпоративной политики надлежащего использования контента и данных.

Средства DLP способны обнаруживать, отслеживать и активно блокировать движение или доступ к конфиденциальным данным, используя ревизию контента и контекстуальные методы анализа для применения одной или нескольких стратегий во время использования. Функции DLP ограничиваются способностью организации определять конфиденциальный контент, его структуру или другие идентифицирующие характеристики.

Данные функции чрезвычайно полезны для ограничения случайного либо вызванного неудовлетворительным ведением бизнеса воздействия. Однако существует множество неконтролируемых процессов, которые могут использоваться злоумышленниками или сотрудниками организации (например, мобильные телефоны с камерами, голосовая почта, бумага и ручка) для обхода систем проверки контента.

Мониторинг приложений и транзакций

Возможности мониторинга приложений и транзакций включают мониторинг приложений, поскольку уязвимости в приложениях зачастую используются для проведения целенаправленных атак, и аномальные действия приложения могут являться единственным признаком мошеннических действий или успешного несанкционированного проникновения в систему. Способность анализировать потоки действий пакетированных приложений позволяет проводить мониторинг этих компонентов на уровне приложений; кроме того, способность определять и анализировать потоки действий со стороны приложений, разработанных по заказу, позволяет проводить мониторинг на уровне приложений в отношении продуктов, разработанных внутри компании.

Функция мониторинга также отслеживает подозрительную активность пользователей в приложении в пределах заданного канала доступа (в том числе через интернет, по телефону или лично либо по приложениям и каналам доступа) или даже организаций, обменивающихся с другими организациями черными списками IP-адресов. Круг задач может быть достаточно широким – начиная с обнаружения аномальных случаев доступа к системе (например, когда одно и то же устройство одновременно подключается из двух удаленных друг от друга точек расположения) и заканчивая вызывающими подозрения цепочками транзакций (например, изменение адреса, за которым следует пересылка крупной денежной суммы). По умолчанию эта функция способна также выявлять несанкционированные действия сотрудников, если они выполняются в рамках приложения, за которым наблюдает служба обнаружения мошеннических операций.

Мониторинг сетевой активности

Возможности мониторинга сетевой активности обеспечивают прозрачность сетевых операций на основе данных о потоках трафика между системами, включая источник, пункт назначения, порт, протокол, обмен передаваемых данных и идентичность пользователя. Данная функция может применяться для выполнения анализа безопасности и связанных с ней операций. Кроме того, этот мониторинг использует комбинацию обнаружения характерных признаков и отклонений для обеспечения прозрачности состояния сети и выявления отклонений от базового уровня, которые могут указывать на аномальную или подозрительную активность. Задача данной функции состоит в том, чтобы организация могла отслеживать свою внутреннюю сетевую активность в целях обнаружения подозрительных действий.

С точки зрения безопасности сценарии использования включают мониторинг в целях обнаружения распространения вирусов-червей, несанкционированной установки приложений и подозрительных действий, связанных с доступом к системе. С точки зрения эксплуатации сценарии использования включают планирование пропускной способности и анализ трафика, в том числе возможность сопоставлять ID пользователя с потоком трафика либо выполнять требования средства контроля по отслеживанию доступа пользователей к критически важным системам. За пределами уровня 3 прозрачность, обеспечиваемая данным мониторингом, невелика, и поэтому он не способен непосредственно обнаруживать проблемы, связанные с доступом к системам, базам данных, контенту, системам файлов и другим объектам.

Мониторинг угроз повышенной сложности

Целенаправленно распространяемые вредоносные программы способны обходить существующие технологии поставщиков услуг интернета (IPS), сетевых брандмауэров и шлюзов веб-безопасности. Сетевые продукты для обнаружения угроз повышенной сложности выпускаются небольшими специализированными фирмами. Принцип работы этих средств основан, как правило, на анализе исполняемых модулей в целях обнаружения вредоносных функций (часто с использованием виртуальных сетевых сред), на мониторинге входящих и исходящих соединений (в том числе запросов DNS (системы доменных имен)) с известными или вызывающими подозрения командно-диспетчерскими пунктами бот-сетей либо на комбинации обоих методов. Возможности данного мониторинга позволяют быстро идентифицировать потенциальную опасность несанкционированного доступа при наличии угроз повышенной сложности (в том числе постоянные угрозы повышенной сложности), однако многими из подобных возможностей дополняются брандмауэры последующих поколений, IPS и шлюзы веб-безопасности.

Задачей других функций является обнаружение угроз безопасности организации со стороны внешнего окружения, в том числе сетей "даркнет", ретранслируемых интернет-чатов, тематических чатов, социальных сетей и т. д. Данные функции могут выполняться путем обнаружения действий в отношении доменов, набора IP-адресов или по определенным ключевым словам.

Управление конфиденциальной информацией и событиями

Возможности управления конфиденциальной информацией и событиями включают широкомасштабный сбор данных о событиях и способность корреляции данных о событиях, полученных из различных источников информации, в целях заблаговременного обнаружения несанкционированного доступа. Данная функция повышает уровень эффективности противодействия угрозам безопасности и эффективности реагирования на инциденты путем сбора и анализа данных о событиях, связанных с безопасностью, из широкого круга источников данных в реальном времени. В число этих источников входят журналы сетевых устройств, приборов системы безопасности, серверов, баз данных и приложений, выходные

данные приложений, связанных с безопасностью, таких как программы управления системой безопасности и действий с базами данных, а также результаты применения соответствующих технологий управления идентичностью и доступом, такие как системы каталогов организаций, регистрации пользователей и управления доступом. Кроме того, данная функция способна осуществлять мониторинг соответствия политике безопасности и расследование инцидентов путем анализа и составления отчетности на основе архивных данных, полученных из этих источников.

Для обнаружения случаев мошенничества рассматриваемая функция группирует и анализирует данные о событиях, выдаваемые устройствами, системами и приложениями. Первичным источником данных служат записи в журнале, однако эта функция способна также обрабатывать и другие формы данных. Данные упорядочиваются таким образом, чтобы события из разных источников могли коррелироваться и анализироваться согласно наборам правил, разработанным для решения конкретных задач, таких как мониторинг событий, связанных с сетевой безопасностью, или мониторинг действий пользователей, поскольку мониторинг и анализ полностью зависят от данных о событиях, выдаваемых другими источниками. Действия, которые не выражены в виде записей в журнале операций или событий, невидимы для данной функции.

8.2 Функциональные возможности обнаружения

Система обнаружения случаев мошенничества использует фоновые серверные процессы (прозрачные для пользователей), изучающие доступ и поведение пользователей. Затем эта информация сравнивается с ожидаемым профилем, который считается нормальным. Одновременно производится оценка комбинации факторов риска, позволяющая выявить реальное мошенничество и снижающая частоту ложного обнаружения. Пользовательские транзакции, вызывающие подозрения, перепроверяются в реальном времени в целях оценки их легитимности или приостанавливаются до тех пор, пока исследованием их легитимности не займутся аналитики по вопросам мошенничества.

Поскольку система обнаружения случаев мошенничества функционирует в рамках приложения, она не может обнаруживать неконтролируемые и потенциально мошеннические процессы, которые являются внешними по отношению к приложению. Система обнаружения случаев мошенничества не может также выявлять подозрительное поведение, для которого у ее механизма отсутствует определение, поскольку правила не учитывают примеры действий, а модель недостаточно обучена для выделения подозрительных действий либо интеграция приложения не обеспечивает достаточного количества данных, необходимых для механизма оценки риска мошенничества. В целях обеспечения эффективности обнаружения для проведения анализа требуется наличие сведений по конкретным сценариям использования либо клиенту необходимо предоставить эти сведения в виде специально заданных правил корреляции и составления отчетов. Следовательно, система обнаружения случаев мошенничества нуждается в таких возможностях, как обновление примеров мошенничества, поддержка библиотек предварительно заданных правил и обработка правил в реальном времени.

Для большинства рассматриваемых возможностей требуется расширенная настройка модели, настройка профиля или разработка правил обнаружения, прежде чем приложения становятся полнофункциональными. Эти возможности включают мониторинг всех транзакций, автоматизированный анализ и определение уровня рисков, составление профиля и изучение поведения пользователей, распознавание интеллектуальных видов мошенничества и мошенничества, обусловленного конкретным видом услуги в данном приложении, а также оценку рисков для всех каналов связи.

Сбор данных о транзакции

Сбор данных о транзакции – это возможности, которые позволяют подбирать и выделять ключевые атрибуты транзакций и требуют автоматического составления подробного профиля поведения для каждого пользователя при первом доступе.

Упорядочение и классификация событий

Данные о событиях должны быть упорядочены таким образом, чтобы события из различных источников могли коррелироваться и анализироваться согласно наборам правил, разработанным для решения специальных задач, таких как мониторинг событий, связанных с сетевой безопасностью, или мониторинг действий пользователей. Это подразумевает сопоставление информации из разнородных источников согласно общей схеме классификации событий. Классификация помогает распознавать примеры, а также расширяет сферу применения и повышает стабильность правил корреляции. Упорядоченные данные из разнородных источников могут быть проанализированы с использованием меньшего количества правил корреляции, что позволяет снизить трудоемкость развертывания и поддержки системы. Кроме того, с упорядоченными событиями проще работать при составлении отчетов и панелей информации.

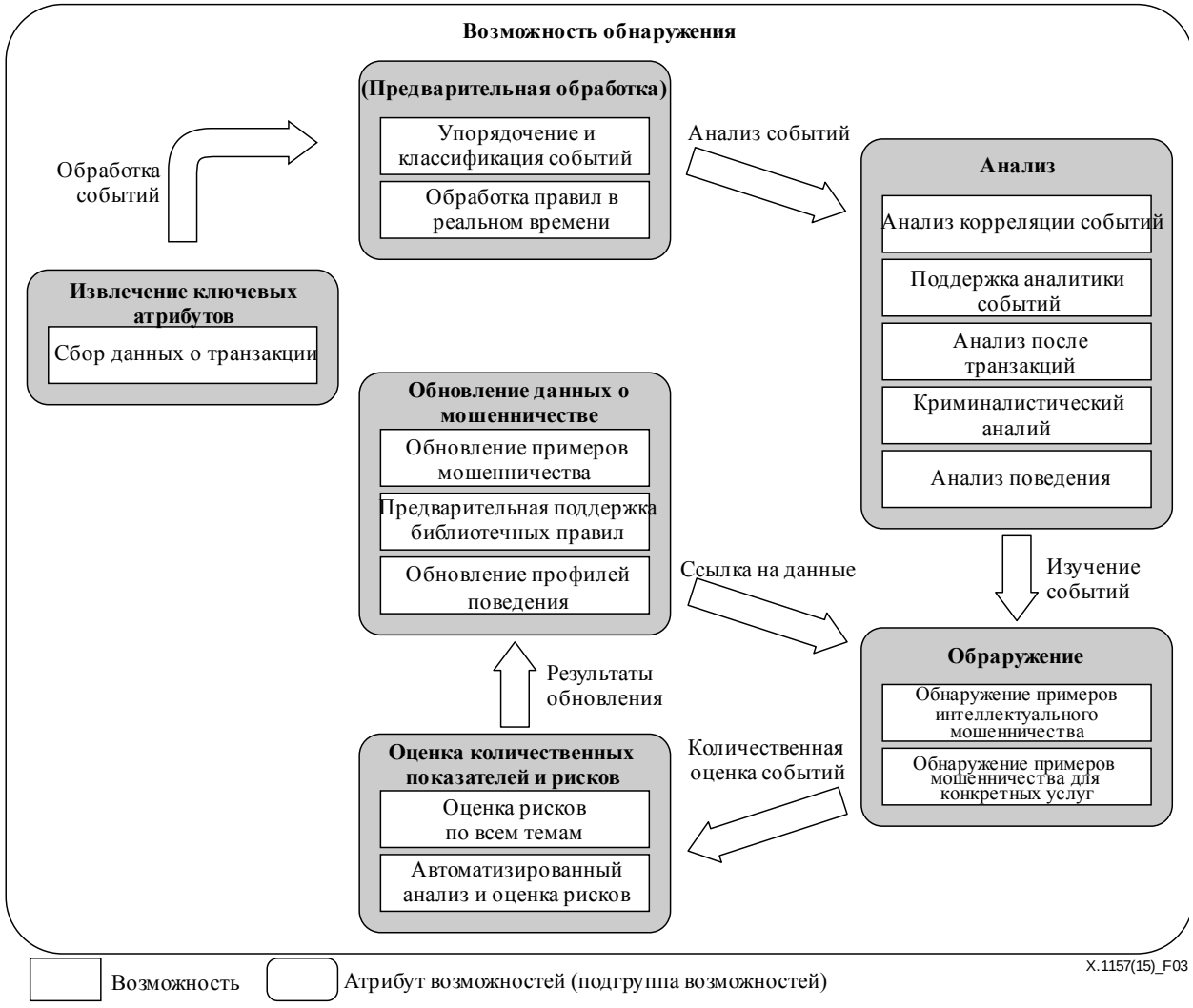

Рисунок 3 – Возможности системы обнаружения мошеннических действий

Обновление примеров мошенничества

Обновление примеров мошенничества – это автоматическое обновление сетевых данных об инцидентах, связанных с мошенничеством. Данные об инцидентах, связанных с мошенничеством, включают информацию о географическом расположении IP-адресов, позволяющую анализировать местонахождение источника транзакций, в том числе город, страну и поставщика интернет-услуг, а также репутационные данные сетевого узла, позволяющие выявлять транзакции из известных сомнительных источников и данные анонимайзеров, в случае если кто-то пытается скрыть исходную точку проведения транзакции. Функция обновления примеров мошенничества должна иметь возможность применения системы обнаружения мошеннических действий в других сценариях ее использования по всей структуре организации и настраивать ее в соответствии с конкретными требованиями, диктуемыми бизнес-интересами организации. К примеру, система обнаружения случаев мошенничества может связывать в одно целое результаты обнаружения мошеннических действий извне, оценку кредитоспособности и интеллектуальные системы совместного использования информации, например черные списки.

Для развертывания системы обновления примеров мошенничества во многих источниках имеется информация о существующих разновидностях сетевых угроз. В число этих источников входят общедоступные списки, базы данных о репутации и угрозах, разработанные и поддерживаемые исследовательскими группами специалистов по безопасности, работающими в компаниях – поставщиках систем безопасности, а также базы данных, разработанные поставщиками систем обеспечения безопасности и других услуг. Информация об угрозах может быть включена в систему обнаружения случаев мошенничества в виде контрольных списков, правил корреляции и запросов при помощи методов, повышающих вероятность успешного и заблаговременного обнаружения несанкционированного доступа.

Актуальная информация о примерах угроз и атак может помочь организации в выявлении аномальных действий. К примеру, отправка данных в небольшом объеме на внешний IP-адрес может показаться вполне нормальной и будет беспрепятственно пропущена. Однако ситуация меняется при наличии разведывательной системы поиска угроз, которая сообщает, что пункт назначения в данной операции связан с управлением бот-сетями. Для обнаружения мошеннических действий эта информация может быть сопоставлена с алгоритмами машинного осмысления предполагаемого поведения либо с более общими правилами в отношении того, какое поведение считать нормальным.

Поддержка предварительно установленных библиотечных правил

Поддержка предварительно установленных библиотечных правил означает, что система обнаружения мошеннических действий поддерживает существующие утвержденные правила для борьбы с мошенничеством. В большинстве случаев данная функция в рамках системы обнаружения мошеннических действий включает ряд утвержденных правил для развертывания системы и должна также задействоваться для упрощения создания/модификации новых правил. Кроме того, данная функция может предусматривать возможность совместного использования правил с другими организациями. Эта функция позволяет системе обнаружения случаев мошенничества быстро обновлять и проверять правила и новые сценарии мошеннических действий, а также без затруднений просматривать и анализировать данные и результаты обнаружения случаев мошенничества. Кроме того, она способна создавать определенный набор правил противодействия мошенническим действиям или злоупотреблениям на уровне клиентов, на уровне групп клиентов или любых других пользователей.

Большинство систем обнаружения мошеннических действий с кредитными картами позволяют предприятиям управлять бизнес-правилами, с которыми они сталкиваются при проведении каждой транзакции. Таким образом, компании могут выявлять примеры мошенничества, применимые к их конкретным ситуациям.

Это библиотечное правило могло бы определять набор правил, основанных на информации, связанной с безопасностью, и контекстуальной информации:

- контекст пользователей – коммерческие функции пользователя;
- контекст ресурсов – форма собственности, сопутствующие приложения или коммерческая деятельность;
- контекст информационной безопасности – существующие уязвимости на уровне операционных систем (ОС), приложений, всемирной сети или баз данных, а также статус конфигурации;
- контекст внешних угроз – известные примеры злоумышленников и атак;
- контекст данных – критически важные для бизнеса или законодательные и нормативные требования;
- контекст приложений – коммерческое использование конкретного приложения и граничные условия для нормального доступа к данным.

Анализ корреляции событий

Корреляция событий устанавливает взаимосвязи между сообщениями или событиями, которые генерируются устройствами, системами или приложениями, на основе таких характеристик, как источник, адресат и протокол или тип события. Кроме того, должны существовать библиотека предварительно установленных правил корреляции и возможность несложной настройки данных правил. При помощи анализа корреляции событий система управления событиями, связанными с безопасностью, должна обеспечивать представление в реальном времени инцидентов и событий, связанных с безопасностью.

Поддержка аналитики событий

Аналитика событий осуществляется путем корреляции событий в реальном времени, а также при помощи анализа прошедших событий, проводимого на основе запросов. Аналитика событий, связанных с безопасностью, включает отображение данных на приборной панели, отчеты и функции незапланированных запросов для поддержки изучения действий пользователя и доступа к ресурсам в целях выявления угроз, несанкционированных проникновений или злоупотребления правами доступа. При выявлении подозрительных действий в результате мониторинга безопасности или сообщений о действиях важно иметь возможность проанализировать пользовательский доступ и доступ к ресурсам. Данный процесс может выполняться при помощи итеративного метода, начиная с расширенного запроса об источнике, пользователе или адресате события, в дальнейшем переходя ко все более узконаправленным запросам, позволяющим выявить источник проблемы. В аналитике событий используются функции поведенческого анализа, дополняющие корреляцию, основанную на правилах.

Обработка правил в реальном времени

Обработка правил в реальном времени – это возможность обработки правил обнаружения мошеннических действий на основании потока транзакций в реальном времени для формирования показателей риска для пользователей и сеансов и подробных оповещений об инцидентах. Данная функция должна учитывать необычное поведение пользователей, общеизвестные примеры мошенничества, черные и белые списки, а также данные

об инцидентах, связанных с мошенничеством. Эта функция может поддерживать синтаксис правил, в том числе необычное поведение пользователей с периодами отсрочки, идентификаторы клиентских устройств, общеизвестные примеры мошенничества, черные и белые списки, данные о местонахождении IP-адресов, а также данные о репутации узла. Кроме того, система обнаружения мошеннических действий может определять показатель риска для каждого сеанса и суммарный показатель риска для каждого пользователя. Система может также поддерживать аутентификацию с учетом рисков, выдавая системе аутентификации в реальном времени показатели рисков для пользователя и сеанса в целях определения необходимости дополнительной аутентификации.

Поддержка средств управления

Данная функция поддерживает экономически эффективное хранение и анализ большого объема информации, включая сбор, индексацию и хранение всех записей журналов и данных о событиях из каждого источника, а также возможность поиска и отчетности по этим данным. Кроме того, функции составления отчетов должны включать заранее определенные отчеты, а также способность составлять специальные отчеты или использовать средства создания отчетов, представленные сторонними разработчиками. Функция средства управления, как правило, включает заранее определенные и изменяемые отчеты по действиям пользователей, доступу к ресурсам, а также образцы отчетов для особых и периодических задач управления. Как правило, средства управления доступны через интернет и поддерживают выделение тех или иных случаев и последовательность операций, в том числе отображение данных по конкретным пользователям, в частности общеизвестного статуса инцидента, связанного с мошенничеством, текущих действий и новых выделенных пунктов, а также настраиваемые механизмы оповещений, включая электронную почту и уведомления веб-служб.

Проведение анализа после транзакции

Функция анализа после транзакции позволяет собирать и хранить все элементы данных для будущего анализа. Впоследствии хранилище данных будет содержать полную историю транзакций для всех пользователей за определенный период времени. Эта функция требует сложного алгоритма сбора и форматирования данных для их хранения в реальном времени и быстрого извлечения и оценки. Система обнаружения мошеннических действий использует профиль поведения каждого отдельного пользователя для проведения анализа после завершения транзакции и способна хранить транзакции, классифицированные по сеансам, пользователям и временным меткам, для последующего извлечения и анализа.

Криминалистический анализ

Функция криминалистического анализа предназначена для поиска, фильтрации и подробного изучения данных о транзакциях, находящихся в хранилище. Она включает возможность фильтрации, поиска и подробного анализа примеров транзакций и доступа. Эта функция поддерживает идентификацию новых примеров мошенничества, для которых должны быть созданы правила обнаружения в реальном времени.

Анализ поведения

Система обнаружения случаев мошенничества требует транзакций с профилями поведения для всех пользователей и поддерживает более сложные системы отслеживания поведения отдельных пользователей. Она формирует профиль нормальной активности и выдает оповещения об отклонениях при помощи функции анализа поведения. Для составления профиля поведения используется этап обучения, на котором создаются профили нормальной активности для отдельных источников событий, собранных при использовании возможностей мониторинга.

Система обнаружения случаев мошенничества автоматически запускает составление профилей пользователей с момента их первого появления в системе. Таким образом, система способна создавать профиль поведения пользователя, которое может считаться нормальным, а затем выявлять необычное поведение по мере его проявления. На этапе обнаружения выдаются оповещения об отклонениях от нормального поведения. Если аномальные условия четко определены, можно задать правила корреляции, согласно которым проводится поиск конкретного набора условий. Эта функция должна быть способна в автоматическом режиме обнаруживать, отслеживать, расшифровывать и разбираться в примерах и аномалиях, которые могут оказаться вредоносными, и при этом не допускать создания помех в работе для законопослушных клиентов. И наконец, составление профиля поведения позволяет оценивать степень риска на основе отклонения от нормального поведения.

В дальнейшем после создания первоначального профиля потребуется больше времени, для того чтобы система определила, какое поведение считается аномальным, а организации смогли ввести в действие надлежащие правила для обнаружения аномального поведения или сеанса. Данный метод может расширить возможности обнаружения целенаправленных атак, однако при этом будет требовать трудоемкой настройки, которая проводится специалистами в данной области и позволяет контролировать появление ложных распознаваний сигналов.

Обнаружение примеров интеллектуального мошенничества

Не все мошеннические действия могут быть обнаружены при помощи журналов сетей и приложений и полей дискретных данных. Анализ неструктурированных данных должен быть включен в состав системы путем использования различных логических процедур интеллектуального анализа данных, которые способны оценить правомерность введенной информации.

Предприятиям следует вести поиск логических систем добычи данных, способных самообучаться на минимальных наборах данных, а также систем, в которых можно легко и быстро обновлять правила для параметров известных или недавно обнаруженных мошеннических действий. Система может проверять идентичность нового онлайнового пользователя, используя услугу количественной оценки идентичности, напрямую предоставляемую поставщиками данной услуги. Эти показатели определяют вероятность того, что онлайновый пользователь является мошенником.

Обнаружение примеров мошенничества для конкретных услуг

Система обнаружения мошеннических действий должна быть способна определять правила, на основе которых производится поиск примеров транзакций, соответствующих известным примерам мошенничества, а также примерам мошенничества, характерным для конкретных услуг. Другими словами, эта система производит поиск определенной последовательности транзакций и условий, которые выглядят подозрительно согласно коммерческим/рабочим логическим процедурам в службе приложений. Данный пример может быть реализован в рамках одного сеанса либо охватывать несколько сеансов и нескольких пользователей, в зависимости от конкретной прикладной услуги.

И наконец, системы обнаружения случаев мошенничества, не настроенные должным образом, могут выдавать слишком много ложных сигналов распознавания. Очевидно, что в таких сферах применения, как электронная торговля, где выполнение транзакций в реальном времени является обязательным, большое количество ложнопозитивных заключений неприемлемо.

Оценка рисков по всем каналам

Системы обнаружения случаев мошенничества функционируют только в заданном приложении и заданном канале и не проверяются по всем каналам (например, телефон, интернет или личное общение) или типам счетов (например, банковский депозит или кредит). Кроме того, системы обнаружения случаев мошенничества не осведомлены о мошеннических действиях за пределами приложения и не встраиваются в системы, обладающие сведениями о подобных действиях (например, системы обнаружения случаев мошенничества на базе сетей или систем). Следовательно, они не могут обнаруживать предосудительные и потенциально мошеннические процессы, которые являются внешними по отношению к приложению.

Соответственно системы обнаружения мошеннических действий требуют наблюдения за активностью подозрительных пользователей в приложении в пределах заданного канала доступа (в том числе через интернет, по телефону или лично) либо по приложениям и каналам доступа или даже организациям (между которыми, к примеру, распространяются черные списки IP-адресов). Круг задач может быть достаточно широким – начиная с обнаружения аномальных случаев доступа к системе (например, когда одно и то же устройство одновременно подключается из двух удаленных друг от друга точек расположения) и заканчивая вызывающими подозрения цепочками транзакций (например, изменение адреса, за которым следует перевод крупной денежной суммы).

Для более эффективного обнаружения мошеннических действий система требует интеграции количественных показателей, полученных от модулей обнаружения случаев мошенничества, в модули оценки степени риска по всем каналам. Эти модули просматривают каналы пользователей (например, центры обработки вызовов или автоматизированные кассовые аппараты (АТМ)).

Автоматизированный анализ и оценка рисков

Данная функция требует возможности оценки, расчета и автоматического определения показателей рисков с точки зрения безопасности. Обнаружение случаев мошенничества и количественная оценка рисков при проведении транзакции выполняются при помощи моделей или правил либо и того и другого вместе. Для обнаружения подозрительной активности на основе различных полученных данных эта функция может использовать альтернативные методы моделирования, в частности байесовские и нейронные сети и другие технологии получения данных. При этом необходимы исходные данные для расчета вероятностей обнаружения мошеннических действий.

Нейронные сети, нормально функционирующие в существующем пространстве кредитных карт, не работают должным образом в интернет-пространстве, поскольку требуют большого объема данных для обнаружения примеров мошеннических действий. В связи с этим в отношении интернет-транзакций система обнаружения случаев мошенничества использует альтернативные методы моделирования, в частности байесовский, который требует меньшего количества данных для расчета вероятностей мошеннических действий или обнаружения случаев мошенничества на основе правил. Модели обнаружения мошеннических действий выдают количественные показатели риска, которые могут быть заложены в наборы правил приложений, а затем будут поддерживаться и обновляться предприятием/организацией.

8.3 Возможности реагирования

Система обнаружения случаев мошенничества требует автоматической выдачи оповещений о мошенничестве, блокирования счетов и более серьезной проверки пользователя, проводящего определенную транзакцию, отмеченную как подозрительная, для функции реагирования на инциденты. Все онлайн-заявления на открытие счета или анонимные транзакции с высоким

уровнем риска должны проходить комплекс процедур начального отбора, начиная с событий, подлежащих идентификации, как результата процедуры начальной проверки подлинности идентичности до использования приложений и журналов приложений. Процедура начального отбора включает основные меры по обнаружению случаев мошенничества, в частности идентификацию клиентского устройства и проверку основных учетных данных, таких как имя, адрес электронной почты, анализ местонахождения, подтверждение телефонного номера, обнаружение мошенничества с кредитными картами, подтверждение отчета из бюро кредитных историй, а также количественная оценка идентичности.

Подозрительные транзакции, которые не прошли начальные этапы проверки подлинности идентичности, должны быть направлены специалистам по расследованию случаев мошенничества и поставлены в очередь на дополнительный анализ в ручном или автоматическом режиме. Впоследствии система обнаружения случаев мошенничества может использовать основанный на степени риска многоуровневый метод проверки подлинности идентичности, который предусматривает усиление проверки идентичности в случае выявления подозрительных пользователей и транзакций с высоким уровнем риска, а также проведение дополнительных проверок.

Усиленная проверка заявителей

Система обнаружения случаев мошенничества может включать механизм аутентификации, с тем чтобы показатель риска, выдаваемый системой обнаружения мошеннических действий, определял эффективность аутентификации пользователя или проверки транзакций, выполняемых пользователем. Данная функция представляет меры, которые могут быть приняты для отсеивания подозрительных транзакций или других транзакций с высоким уровнем риска, требующих проверки идентичности. Для обеспечения минимальных затрат и максимального удобства клиентов предприятия могут применять метод, основанный на уровне риска, в котором эффективность механизма проверки идентичности соразмерна с риском, представляемым транзакцией. Для этого система обнаружения мошеннических действий может использовать комбинацию из нескольких приложений проверки идентичности, описанных в документе [b-ITU-T X.1154].

В целом на рынке не существует единого универсального приложения для проверки идентичности. Однако имеется ряд коммерческих механизмов проверки идентичности, которые могут сочетаться, предоставляя эффективный сдерживающий фактор против мошенников.

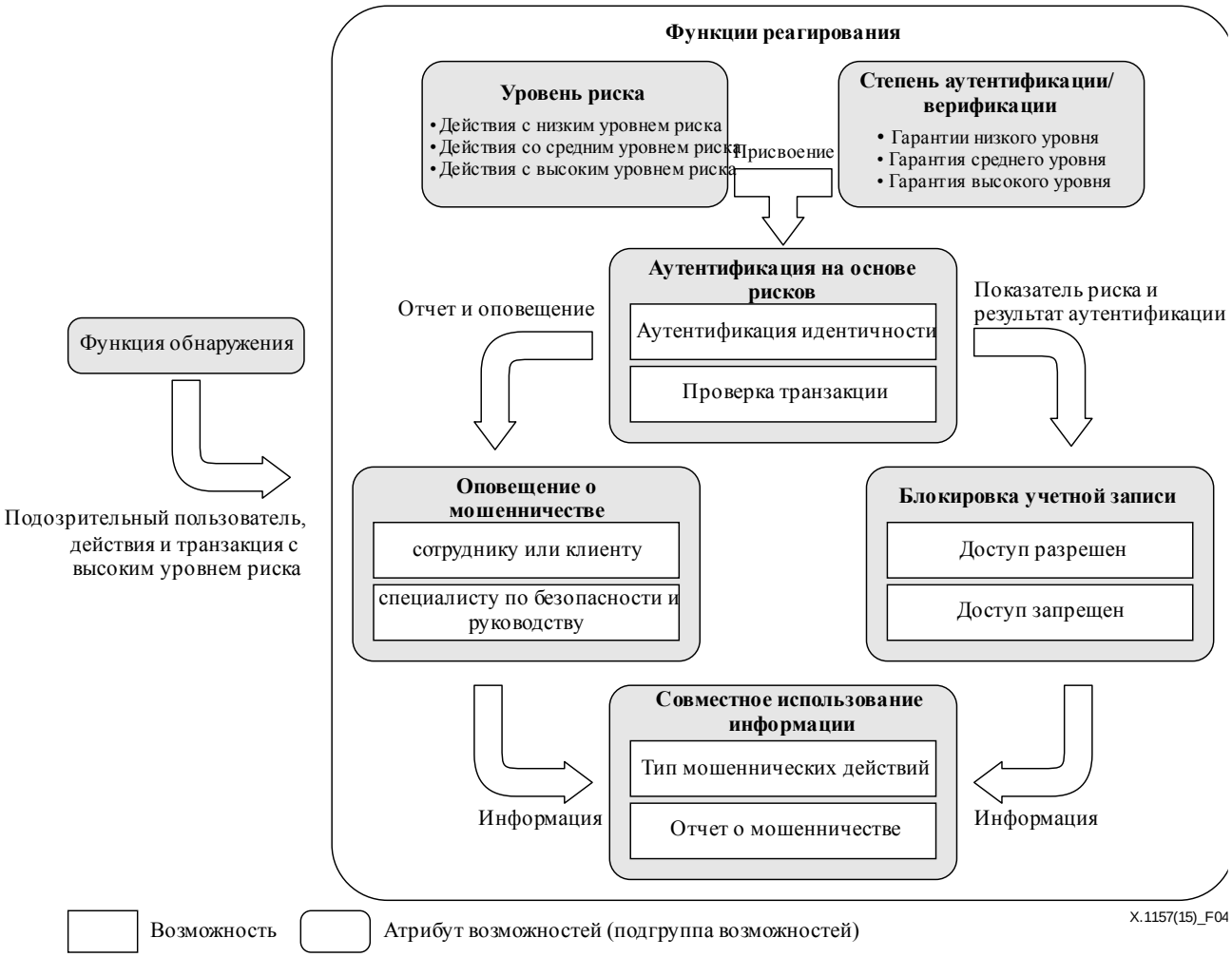

Рисунок 4 – Возможности реагирования системы обнаружения мошеннических действий

Аутентификация на основе рисков

Чем выше уровень риска, определенный, например, системой обнаружения случаев мошенничества, тем более затратными и неудобными для клиентов могут оказаться меры по проверке подлинности идентичности. Существует несколько методов, при которых требуется более серьезная аутентификация, например:

- для проведения операций с низким уровнем риска, таких как доступ к публичной информации в режиме "только для чтения", устанавливается начальный уровень доступа к учетной записи, требующий лишь простейшей проверки подлинности идентичности. Например, механизм проверки подлинности идентичности может проверять имя пользователя и почтовый адрес по вторичному источнику;
- операции с высоким уровнем риска, в частности изменение почтового адреса, приостанавливаются до тех пор, пока наряду с мерами по обнаружению мошеннических действий не будет проведена более серьезная проверка подлинности идентичности
  (см. [b-ITU-T X.1254]). Такая проверка включает аутентификацию, обеспечивающую более высокий уровень гарантии:
  – механизм проверки подлинности идентичности может удостоверять личные данные по базе общедоступных источников информации, используя

аутентификацию на основе сведений. В ходе проверки объединяется общедоступная информация, например демографические данные, информация из базы водительских удостоверений и данные, полученные из бюро кредитных историй;

– механизм проверки подлинности идентичности может потребовать от пользователя ответить на один или несколько сложных вопросов, ответы на которые либо заранее определены, либо сохранены в профиле пользователя, либо основаны на информации, известной только подлинному владельцу учетной записи;

– механизм проверки подлинности идентичности также может использовать альтернативные методы аутентификации канала, такие как номер сотового телефона или адрес электронной почты, позволяющие связаться с владельцем учетной записи. Механизм проверки подлинности идентичности может отправлять одноразовый пароль новому онлайн-пользователю при помощи голосового вызова или SMS-сообщения на телефонный номер, зарегистрированный в организации или введенный пользователем при подаче нового заявления об открытии счета или на странице платежа;

• наиболее рискованные операции, такие как денежные переводы на привязанный внешний банковский счет, запрещены до тех пор, пока пользователь при контакте не подтвердит их. Однако поскольку многие транзакции выполняются в пакетном режиме (а не в реальном времени), при применении этого метода срок выполнения транзакции может не меняться.

Оповещения о мошенничестве

Оповещения о мошенничестве – это автоматическая/ручная выдача оповещения при обнаружении подозрительной активности. Оповещение о мошенничестве, как правило, является результатом объединения количественного показателя рисков и некоторых правил, действующих на основе этого показателя. Подробные оповещения включают атрибуты транзакций и описание действий и могут быть направлены по электронной почте и при помощи устройства персонального вызова (пейджера). Данный процесс регулируется действующими правилами, степенью опасности и управляющими пользователями. Оповещения о мошенничестве могут направляться специалистам по безопасности или клиентам/пользователям в зависимости от измеренного уровня риска. Специалист по безопасности может впоследствии более подробно исследовать уровень риска, а оповещение о мошенничестве, направленное клиенту/пользователю, может использоваться для предупреждения потенциальных кредиторов о том, что их идентификационная информация возможно украдена.

Блокировка учетных записей

Блокировка учетных записей пользователей применяется при обнаружении подозрительной активности. Пользователь может получить разрешение или отказ в доступе на основании присвоенного рейтинга и пределов допуска, установленных в организации. Пользователям, рейтинг которых недостаточен для предоставления полного доступа, может быть предоставлен ограниченный доступ либо им потребуется пройти более серьезную аутентификацию для получения полного доступа или разрешения на выполнение определенных транзакций с высоким уровнем риска. Пользователи, не соответствующие этим требованиям, могут повторно подвергаться процедуре усиленной проверки либо их учетные записи немедленно блокируются.

Совместное использование информации

Системы обнаружения случаев мошеннических действий должны обеспечить эффективную координацию этапов их деятельности, связанной с реагированием на инциденты, с соответствующими партнерами организации.

Наиболее важным аспектом координации деятельности по реагированию на инциденты является совместное использование информации, когда различные организации обмениваются друг с другом данными об угрозах, атаках и уязвимостях, благодаря чему сведения, имеющиеся у одной из организаций, приносят пользу другим. Кроме того, совместное использование информации может осуществляться напрямую между предприятием и клиентами или между организаций и сотрудниками, поскольку одни и те же угрозы или атаки зачастую затрагивают несколько организаций или служб одновременно. При совместном использовании информации любая организация, обнаружившая мошенничество, делится данной информацией как внутри собственной структуры, так и с другими организациями, которые могут стать жертвами мошенников.

Организация-получатель может использовать данную информацию, например, для назначения ручного просмотра транзакций, выполняемых с подозрительных IP-адресов. Отчет о мошеннических действиях может описывать конкретную транзакцию, которая известна как мошенническая или предполагается таковой, а также может описывать пример действий, который, как предполагается, является признаком мошенничества.

Дополнение I

Прикладные услуги ИКТ, требующие защиты

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Электронные финансовые услуги

I.1.1 Электронные банковские услуги и вопросы обеспечения безопасности

Онлайновые банковские услуги (интернет-банкинг или электронные банковские услуги) позволяют клиентам финансовых учреждений осуществлять финансовые транзакции посредством надежного веб-сайта, находящегося в ведении данного учреждения, которым может быть розничный или виртуальный банк, кредитный союз или строительная компания. Для осуществления онлайн-доступа к банковским услугам финансового учреждения клиент, имеющий персональный доступ в интернет, должен зарегистрироваться в учреждении и установить пароль (под уникальным именем) для проверки идентичности клиента. Для осуществления доступа к онлайновым банковским услугам клиенту следует зайти на веб-сайт финансового учреждения и подключиться к онлайновым банковским операциям, используя номер и пароль клиента. Некоторые финансовые учреждения установили дополнительные меры безопасности при осуществлении доступа к онлайн-услугам, однако применяемый подход не имеет системного распространения.

Хотя аутентификация по одному паролю до сих пор используется, в некоторых странах она не считается достаточно безопасной для пользования онлайновыми банковскими услугами. Для обеспечения безопасности при использовании онлайновых банковских услуг применяются два метода.

- В системе на основе личного идентификационного номера/номера транзакции (PIN/TAN) PIN-код представляет собой пароль, используемый для входа в систему, а TAN – это одноразовые пароли для подтверждения транзакций. Распределение номеров транзакций (TAN) может осуществляться различными способами. Наиболее распространенный – это отсылка списка номеров TAN пользователю онлайновых банковских услуг письмом по почте. Наиболее безопасный способ использования номеров TAN – это их генерация по мере необходимости при помощи секретного ключа. В этом случае номера TAN генерируются при помощи ключа в зависимости от времени и уникального секретного кода, хранящегося в секретном ключе (двухфакторная аутентификация). Оказание онлайновых банковских услуг с помощью номеров PIN/TAN обычно осуществляется через веб-браузер с использованием защищенных соединений по протоколу безопасных соединений (SSL), благодаря которому отсутствует необходимость дополнительного шифрования.
- Еще одним способом передачи номеров TAN пользователю онлайновых банковских услуг является отправка сообщения SMS с номером TAN текущей банковской транзакции на мобильный телефон пользователя, работающий по стандарту GSM (глобальная система подвижной связи). В тексте SMS обычно приводится сумма и подробная информация о транзакции; номер TAN является действующим лишь на короткое время. Услуга "TAN через SMS" используется в банках многих стран, в частности Германии, Австрии и Нидерландов, так как считается, что данный способ обеспечивает высокий уровень безопасности.
- Существует разновидность онлайн-банкинга на основе подписи, в которой все транзакции заверяются цифровой подписью и шифруются. Ключи для генерации

подписи и шифрования могут храниться на смарт-картах или на любом другом запоминающем устройстве в зависимости от конкретной системы реализации.

I.1.2 Электронные платежи и вопросы безопасности

Электронный платеж – это обмен или передача денежных средств с одного счета на другой, осуществляемый электронным способом, либо внутри одного финансового учреждения, либо между несколькими финансовыми учреждениями при помощи компьютерных систем.

Система незащищенных электронных платежей может не пользоваться доверием среди клиентов. Доверие имеет чрезвычайно большое значение для признания системы пользователями. Проблема безопасности характерна для приложений с электронными платежами, так как они в значительной степени зависят от критически важных систем ИКТ, которые являются причиной уязвимостей финансовых учреждений и предприятий и потенциально могут нанести вред клиентам. Безопасная электронная финансовая транзакция должна удовлетворять следующим требованиям.

- Целостность и авторизация. Под целостностью понимается точность, полнота и достоверность информации в соответствии с корпоративными ценностями и ожиданиями. Целостность систем платежей означает, что снятие каких-либо финансовых средств невозможно без разрешения пользователя на проведение платежа. Кроме того, пользователи вправе потребовать от финансового учреждения не принимать от них каких-либо платежей без их явно выраженного согласия.
- Конфиденциальность. Конфиденциальность определяется как защита секретной или частной информации от несанкционированного раскрытия. Некоторые из сторон-участников могут потребовать конфиденциальности транзакций. Конфиденциальность в данном контексте означает ограничение доступа к различной информации, относящейся к транзакции, например идентичности плательщика/получателя платежа, содержимого и объема покупки и т. д. В большинстве случаев стороны-участники желают убедиться в том, что связь является конфиденциальной.
- Готовность и надежность. Готовность – это гарантия того, что информационные системы и данные могут использоваться тогда, когда это потребуется. Готовность часто выражается в процентах времени, в течение которого система может быть использована для продуктивной работы. Все стороны требуют наличия возможности совершать или получать платежи в случае любой необходимости.

I.2 Услуги электронного здравоохранения

Электронное здравоохранение, предусматривающее безбумажное управление всей деятельностью крупных медицинских учреждений, обещает широкие перспективы по ускорению бюрократических процедур, типичных для здравоохранения в медицинских центрах и больницах. Однако в реальности надлежащее развитие электронного здравоохранения сталкивается со множеством проблем, связанных с безопасностью. Для широкого использования электронного здравоохранения в больницах необходима детальная проработка вопросов безопасности и подготовка к стандартизации различных компонентов системы для надлежащего развития электронного здравоохранения. Типичная система электронного здравоохранения может включать многие компоненты и подсистемы, такие как расписание и время приема врача; поступление в больницу, выписка и перевод; назначение лечения; планирование режима питания; записи в медицинских картах; лабораторные и рентгеновские анализы; архивация снимков и ввод смарт-карт. Каждая из этих подсистем уязвима в плане безопасности.

I.2.1 Вопросы безопасности при оказании услуг в сфере электронного здравоохранения

- Угрозы для конфиденциальности личных данных и информационной безопасности. Существующая база знаний по рискам для информационной безопасности позволяет выделить различные типы угроз конфиденциальности и информационной безопасности в сфере здравоохранения. Однако существующая на данный момент специальная классификация сама по себе может оказаться не вполне практичной.
- Проблемы защиты личной информации пользователей системы здравоохранения. Активизация использования систем на базе интернет-технологий для управления медицинской информацией и введения в действие банков данных персонального медицинского обслуживания вывела на передний план вопросы защиты личных данных пользователей системы здравоохранения.
- Функциональная совместимость данных и информационная безопасность. Основной предпосылкой функциональной совместимости данных является упрощение точной и бесперебойной передачи информации внутри учреждения и между учреждениями для обеспечения своевременного оказания медицинской помощи.
- Вопросы информационной безопасности электронного здравоохранения. Для сферы здравоохранения характерен значительный рост использования мобильных устройств и веб-приложений. В то же время исследования в области информационной безопасности посвящены развитию структуры и протоколов для решения вопросов безопасности в электронном здравоохранении.

I.3 Услуги корпоративного удаленного доступа

Сотрудники и контрагенты многих организаций, работающие за пределами их расположения, используют технологии корпоративного удаленного доступа. Большинство сотрудников, работающих на дому с ПК, используют методы корпоративного удаленного доступа для связи с внутренними вычислительными ресурсами организации. Основная характеристика технологий корпоративного удаленного доступа – предоставление доступа к защищенным ресурсам из внешних сетей, а зачастую также из внешних сетевых узлов. Эти ресурсы, как правило, подвергаются гораздо большему риску, чем при использовании аналогичных технологий, доступных только внутри организации. Кроме того, возрастает риск для внутренних ресурсов, к которым работающие на дому получают доступ посредством корпоративного удаленного доступа.

I.3.1 Проблемы безопасности корпоративного удаленного доступа

Наиболее распространенными показателями, связанными с безопасностью технологий корпоративного удаленного доступа, являются:

- конфиденциальность – обеспечение защиты соединений удаленного доступа и сохраненных пользовательских данных от несанкционированного прочтения;
- целостность – обнаружение любых преднамеренных или непреднамеренных изменений в соединениях удаленного доступа, происходящих при пересылке данных;
- доступность – обеспечение возможности удаленного доступа пользователей к ресурсам в любой момент по мере необходимости.

Для достижения этих показателей все компоненты систем корпоративного удаленного доступа, включая клиентские устройства, серверы удаленного доступа и внутренние серверы, подключаемые через удаленный доступ, должны быть защищены от различных сетевых угроз. Технологии корпоративного удаленного доступа часто нуждаются в дополнительной защите,

поскольку они по сути своей в большей степени подвержены внешним угрозам, чем технологии, доступ к которым осуществляется только в пределах организации.

Ниже указаны основные проблемы, связанные с безопасностью корпоративного удаленного доступа.

- Отсутствие физического контроля безопасности. Клиентские устройства корпоративного удаленного доступа используются в самых разных местах вне зоны контроля организаций, например дома у сотрудников, в кофейнях, гостиницах и конференц-залах. Мобильность этих устройств повышает вероятность их утери или кражи, в связи с чем риск рассекречивания данных, хранящихся на устройствах, достаточно велик. Даже в том случае, если клиентское устройство постоянно находится в руках владельца, существуют другие физические риски для безопасности, например, злоумышленник может заглянуть через плечо сотрудника предприятия, использующего корпоративный удаленный доступ в кофейне, и просмотреть конфиденциальные данные на экране клиентского устройства.
- Незащищенные сети. Поскольку почти всегда корпоративный удаленный доступ осуществляется через интернет, организации, как правило, не могут контролировать безопасность внешних сетей, используемых клиентами. Системы связи, которые используются для корпоративного удаленного доступа, включают телефонные модемы, модемы цифровых абонентский линий (DSL), широкополосные сети, в том числе кабельные и беспроводные средства (см. [b-IEEE 802.11]), технологию сети всемирной функциональной совместимости для микроволнового доступа (WiMAX) и сотовые сети. Эти системы связи уязвимы для прослушивания, которое подвергает риску рассекречивания конфиденциальную информацию, передаваемую через систему корпоративного удаленного доступа. Для перехвата и модификации соединений могут также проводиться атаки типа "человек посередине" (MITM). Риск использования незащищенных сетей может быть снижен (но не устранен совсем) при помощи технологий шифрования для защиты конфиденциальности и целостности соединений, а также при помощи использования механизмов взаимной аутентификации для проверки идентичности обеих оконечных точек.
- Зараженные вирусами устройства, подключенные к внутренним сетям. Клиентские устройства, особенно ноутбуки, часто используются во внешних сетях, а затем приносятся в организации и подсоединяются напрямую к их внутренним сетям. Злоумышленник, имеющий физический доступ к клиентскому устройству, может установить на него вредоносные программы, предназначенные для извлечения данных как из самого устройства, так и из сетей и систем, к которым оно подключается. Если клиентское устройство заражено вредоносными программами, то они могут распространиться по организации сразу после того, как клиентское устройство подключится к внутренней сети. Помимо использования соответствующих антивирусных технологий, входящих в базовую конфигурацию системы безопасности организации, в том числе антивирусного программного обеспечения на клиентских устройствах, в организациях должны быть предусмотрены системы контроля доступа к сети (NAC), которые проверяют возможности обеспечения безопасности клиентского устройства, прежде чем разрешить ему использовать внутреннюю сеть. Организации должны также предусмотреть использование отдельной сети для клиентских устройств сотрудников, работающих на дому, вместо того чтобы позволять им напрямую подключаться к внутренней сети.
- Внешний доступ к внутренним ресурсам. Система корпоративного удаленного доступа предоставляет внешним сетевым узлам доступ к внутренним ресурсам, например к серверам. Если до этого внутренние ресурсы были недоступны из внешних

сетей, то подключение к ним через удаленный доступ создает новые угрозы, особенно со стороны ненадежных клиентских устройств и сетей, и значительно повышает вероятность того, что данные будут рассекречены. Каждый вид корпоративного удаленного доступа, который может использоваться для доступа к внутренним ресурсам, повышает риск рассекречивания информации на этом ресурсе.

Библиография

[b-ITU-T X.1141] Рекомендация МСЭ-Т X.1141 (2006 год) *Язык разметки, предусматривающий защиту данных (SAML 2.0)*

[b-ITU-T X.1154] Рекомендация МСЭ-Т X.1154 (2013 год) *Общая структура комбинированной аутентификации в среде с несколькими поставщиками услуг определения идентичности*

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 год) *Базовые термины и определения в области управления определением идентичности*

[b-ITU-T X.1254] Рекомендация МСЭ-Т X.1254 (2012 год) *Структура гарантии аутентификации объекта*

[b-IEEE 802.11] IEEE 802.11, *IEEE Standard for Information technology – Telecommunications and information exchange between systems, Local and metropolitan area network – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2016 год