
R·Vision
At the root of your security

Обмен информацией об угрозах и инцидентах информационной безопасности

Александр Бондаренко, CISA, CISSP
Генеральный директор, R-Vision

Февраль 2018

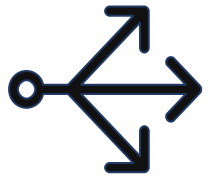
Обмен информацией

неотъемлемая часть ИБ

Исходящий

Партнеры | Регуляторы

Входящий



Исходящая информация

Основные нормативы

Новая редакция 382-П (вступит в силу с 1 июля 2018г.)

Регламент обмена информацией с ФинЦЕРТ

187-ФЗ и подзаконные акты

Номер строки	Дата выявления инцидента	Наименование банковского платежного агента (субагента)	Код банковского платежного агента (субагента) по ОКПО	Регистра-ционные номера операторов платежных систем	Последствия инцидента	Объекты информа-ционной инфраст-руктуры	Описание предпринятых действий по устранению последствий инцидента	Факт обра-щения в правоохра-нительные органы
1	2	3	4	5	6	7	8	9

Раздел 3. Сведения об инцидентах отчетного периода

Номер строки	Тип инцидента	Дата выявления инцидента, дата возникновения инцидента	Условия возникновения инцидента	Описание инцидента	Причина инцидента	Дополнительные сведения об инциденте	Регион возникновения инцидента	Нарушенное требование Положения Банка России N 382-П	Отношение к платежной системе	Последствия инцидента			Описание предпринятых действий по устранению последствий инцидента	Факт обращения в правоохранительные органы	Сведения о выявлении инцидента клиентом, банковским платежным агентом (субагентом), операционным центром, находящимся за пределами Российской Федерации	Код банковского платежного агента (субагента)	Дата завершения разбирательст по инцидент
										Суммы переводов денежных средств	Нарушение сроков	Оценка убытка					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2.1	02.01.2014,02.01.2014	4.9	5.6,5.7	6.7,6.8		45	П.9,П.10,П.13	0004		05.45	345000	Замена (перевыпуск) платежной карты клиента Корректировка настроек средств защиты информации	15.3			21.01.2014
2	2.2	14.01.2014,14.01.2014	4.2,4.11.5	5.5,5.7	6.7,6.9		45268	П.4,П.20,П.29.2	0006	399000,39000		450000	Привлечение сторонней организации для проведения расследования инцидента ИБ	15.7	БПА №1	34342	31.01.2014
3	2.3	17.01.2014,16.01.2014	4.3	5.7,5.8	6.10		45	П.6,П.25,П.36	0001	345000		219000	Корректировка настроек средств защиты информации	15.6	Коммерческий банк "Анелик РУ" (Общество с ограниченной ответственностью), ООО КБ "Анелик РУ"		

Необходимые действия

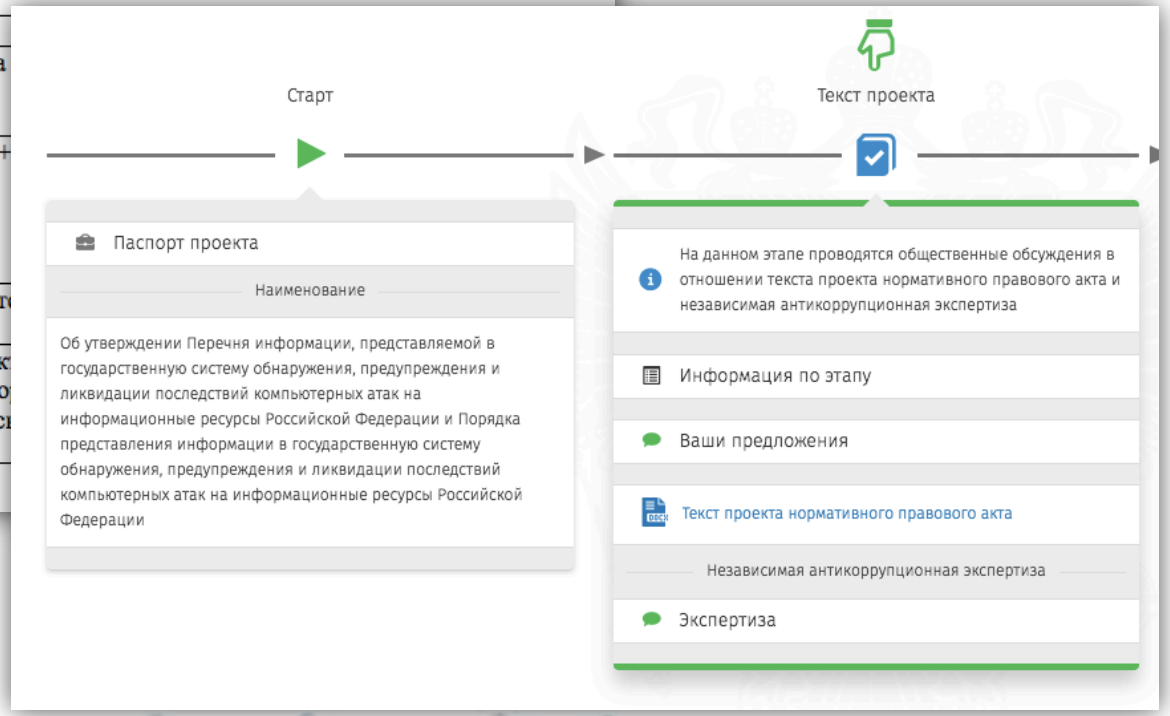
№1 Понять объем необходимых сведений

КАРТОЧКА – Код PUB

Информация о планируемых мероприятиях по раскрытию информации об инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, включая размещение информации на официальных сайтах в информационно-телекоммуникационной сети «Интернет», выпуск пресс-релизов и проведение пресс-конференций.

2. Общие сведения, содержащиеся в карточках инцидентов кода INT и EXT

№ п\п	Содержание	Примечание
1	Название участника информационного обмена (полное)	Указывается полное официальное наименование участника
2	Контактные данные ответственных лиц участника информационного обмена (обязательно)	Указывается ФИО, должность, номер телефона в формате + электронной почты
3	Дата и время выявления инцидента (обязательно)	Дата указывается в формате ГГГГММДД. Время указывает в формате UTC+X (например, для Москвы: UTC + 3)
4	Место выявления (обязательно)	В соответствии с Общероссийским классификатором объек (ОКАТО) указывается первый уровень классификации в фо **В случае выявления инцидента с кодом (EXT)&(CBR),** с денежных средств **поле не заполняется**



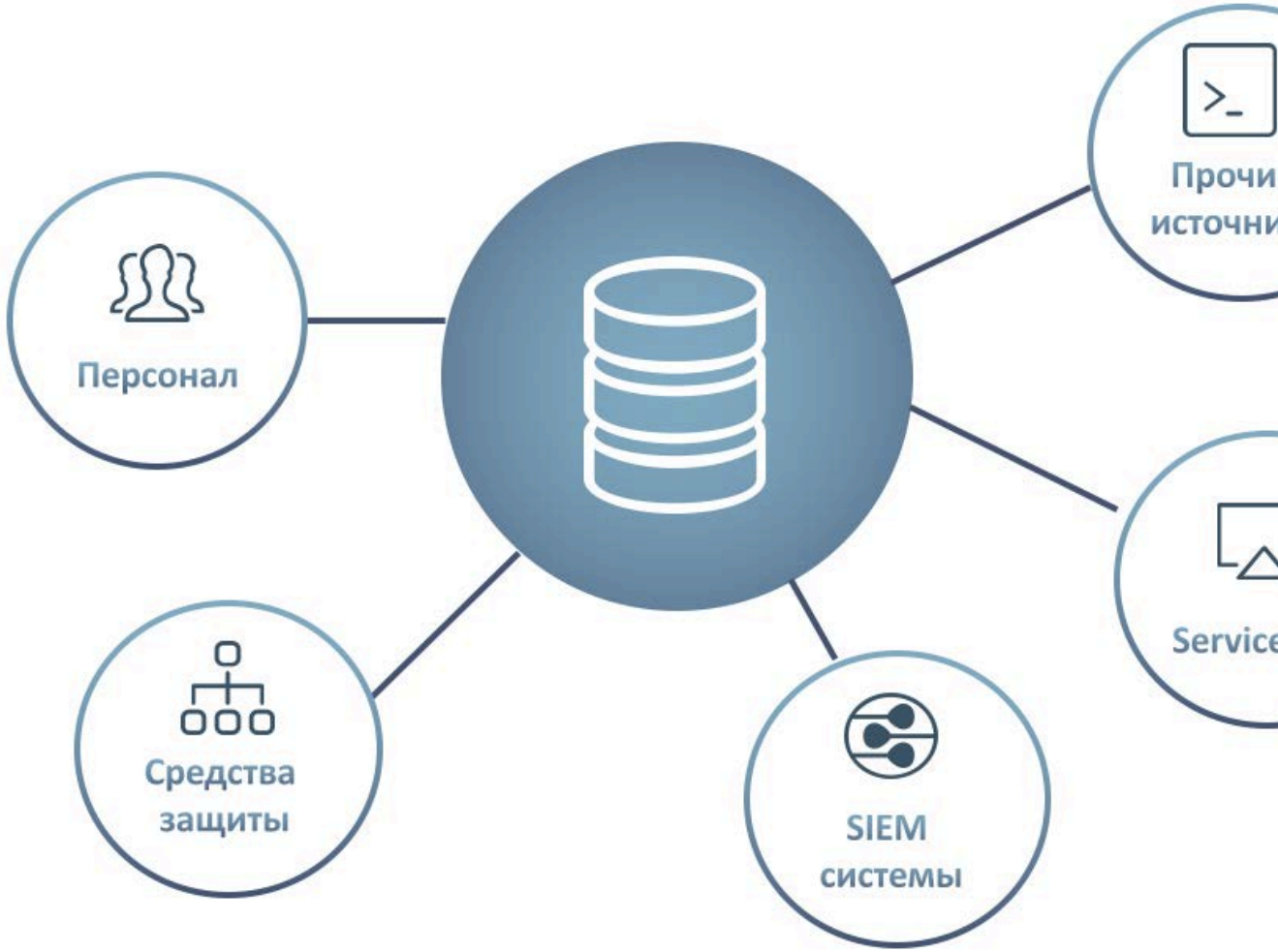
№2 Определить источники информации

Персонал

Средства защиты

ИТ/ Бизнес-системы

Аутсорсеры

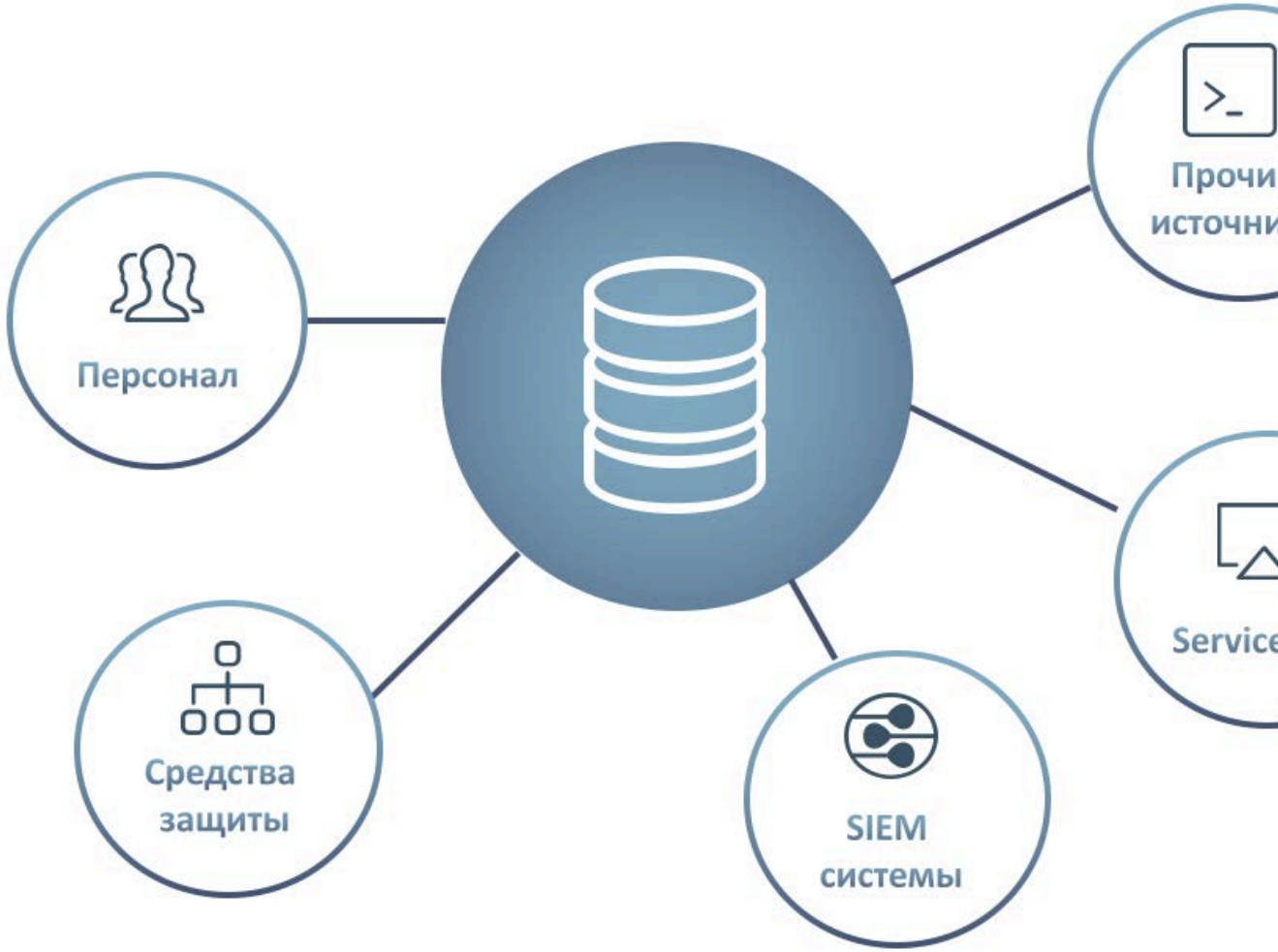


№3 Обеспечить централизованный сбор

Интеграции с другими системами

Парсинг сообщений

Веб-формы

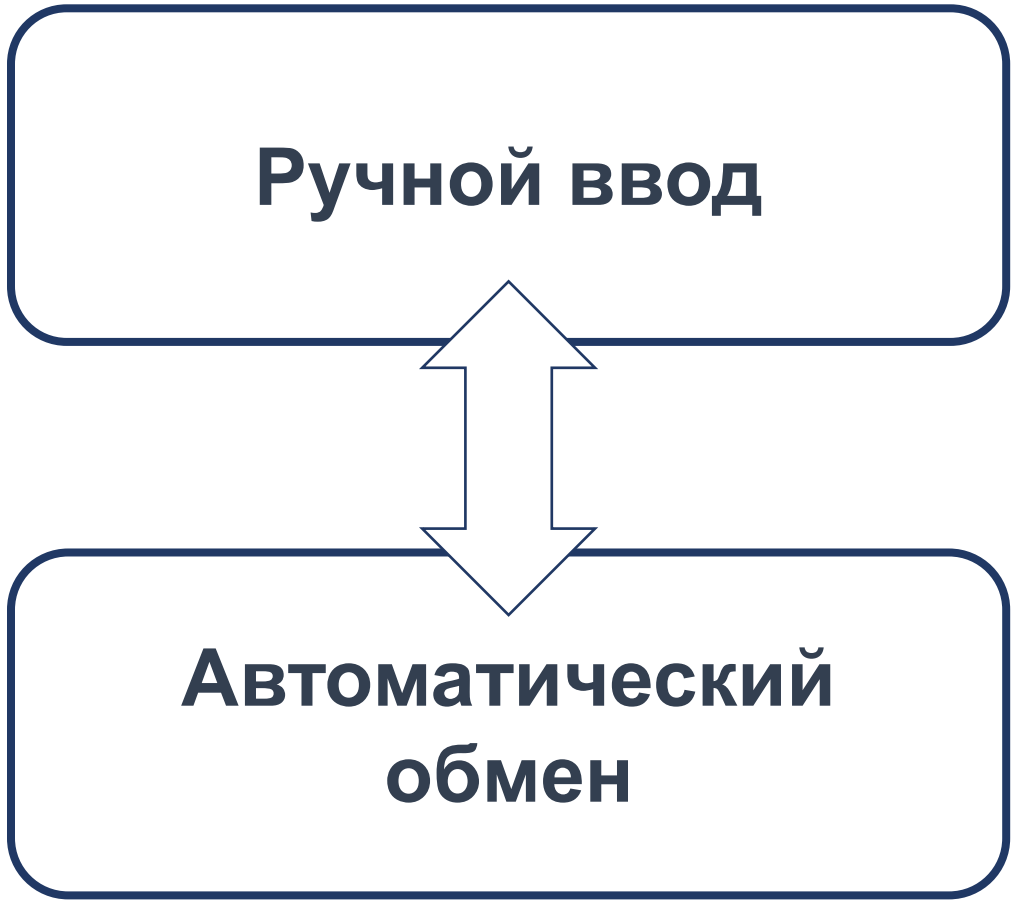


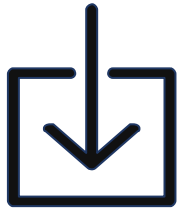
№4 Согласовать механизмы обмена

Электронная почта
Файлы

Программные интерфейсы (API)

Веб-интерфейсы





Входящая информация

Источники данных

ФинЦЕРТ | SWIFT | IBM X-Force | AlienVault | Kaspersky …

ФИНЦЕРТ | PC-V-BN-20180130-01

Предупреждение! Зафиксирована рассылка ВПО!

1. Краткое описание угрозы

Зафиксированы факты распространения модификации вредоносного программного обеспечения «Dimnie» с перечисленных ниже адресов в сети Интернет. Предположительно, осуществляется атака на организации кредитно-финансовой сферы.

2. Основные индикаторы компрометации

№	Тип IOC	Список
1	URL-адреса и IP-адреса, к которым производятся обращения	worldmed[.]bit ryhesheheghow[.]online 54.236.38[.]98 185.82.217[.]244
2	Адреса и домены отправителей писем	dir@vektor-mebel[.]com

Ниже приведены данные по известным файлам из рассылки.

Информацию об обнаружении файлов антивирусными средствами различных производителей вы можете получить, например, по данным сайта virustotal.com, введя в поле поиска соответствующие файлам хэш-суммы, либо обратившись в техническую поддержку вендора использующегося в вашей

Источники данных

ФинЦЕРТ | SWITF | IBM X-Force | AlienVault | Kaspersky …

ФИНЦЕРТ PC-V-BN-2

Предупреждение! Зафикси

1. Краткое описание угроз

Зафиксированы факты р
программного обеспечения «Di
Интернет. Предположительно, о
финансовой сферы.

2. Основные индикаторы к

№	Тип IOC
1	URL-адреса и IP-адреса, к которым производятся обращения
2	Адреса и домены отправителей писем

Ниже приведены данные по

Информацию об обнар
различных производителей вы можете получить, например, по данным сайта virustotal.com, введя в поле поиска соответствующие файлам хэш-суммы, либо обратившись в техническую поддержку вендора использующегося в вашей

Home › News & Events › News › SWIFT launches the 'SWIFT Information Sharing and Analysis Centre'

15 May 2017

SWIFT launches the 'SWIFT Information Sharing and Analysis Centre'

The latest development on cyber-security information sharing is part of SWIFT's Customer Security Programme

SWIFT is pleased to announce the launch of the 'SWIFT Information Sharing and Analysis Centre' (SWIFT ISAC) global portal which is now available to the SWIFT community.

The new SWIFT ISAC portal stores all the valuable information SWIFT has been sharing with the SWIFT community through KB Tips in our existing Knowledge Base on swift.com. All the related and existing intelligence bulletins will now be stored in the SWIFT ISAC portal, in a readily readable and searchable format, aligned with standardised templates.

This information includes malware details such as file hashes and YARA rules, Indicators of Compromise, as well as details on the Modus Operandi used by the cyber-criminals. The information, which is particularly relevant to SWIFT customers, can also be downloaded as PDF reports or as machine-readable files in OpenIOC format, an XML-based file format that is commonly used by the cyber-security industry.

Источники данных

ФинЦЕРТ | SWITF | IBM X-Force | AlienVault | Kaspersky …

ФИНЦЕРТ PC-V-BN-2

Предупреждение! Зафикси

1. Краткое описание угроз

Зафиксированы факты р
программного обеспечения «Di
Интернет. Предположительно, о
финансовой сферы.

2. Основные индикаторы к

№	Тип IOC
1	URL-адреса и IP-адреса, к которым производятся обращения
2	Адреса и домены отправителей писем

Ниже приведены данные по

Информацию об обнар
различных производителей вы можете получить, например, по д
virustotal.com, введя в поле поиска соответствующие файлам хэш-
обратившись в техническую поддержку вендора использующего

Home › News & Events › News › SWIFT launches the 'SWIFT Information Sharing and Analysis Centre'

15 May 2017

SWIFT launches the 'SWIFT Information Sharing and Analysis Centre'

The latest development on cyber
Customer Security Programme

SWIFT is pleased to announce the laur
(SWIFT ISAC) global portal which is no

The new SWIFT ISAC portal stores all t
community through KB Tips in our exis
intelligence bulletins will now be stored
format, aligned with standardised temp

This information includes malware deta
Compromise, as well as details on the
which is particularly relevant to SWIFT
machine-readable files in OpenIOC for
cyber-security industry.

IBM **X-Force Exchange** Create IBMid Log In

Research, Collaborate and **Act** on threat intelligence

Search by Application name, IP address, URL, Vulnerability, MD5, #Tag... …or Scan file

Trending

199.59.242.150 103.224.212.222
#malware 198.54.117.200
[object object] am i affected
#threat-actor #phishing

Dashboard

AlertCon™ Threat Level 1

Recent IBM X-Force Advisories
Collections created by the IBM X-Force team

- Lazarus Group Returns With New Targets
  Feb 15, 2018 - incident
- Olympic Destroyer
  Feb 13, 2018 - malware
- LuminosityLink Apparently Dead

Threat Activity
Malicious IP addresses in the last hour

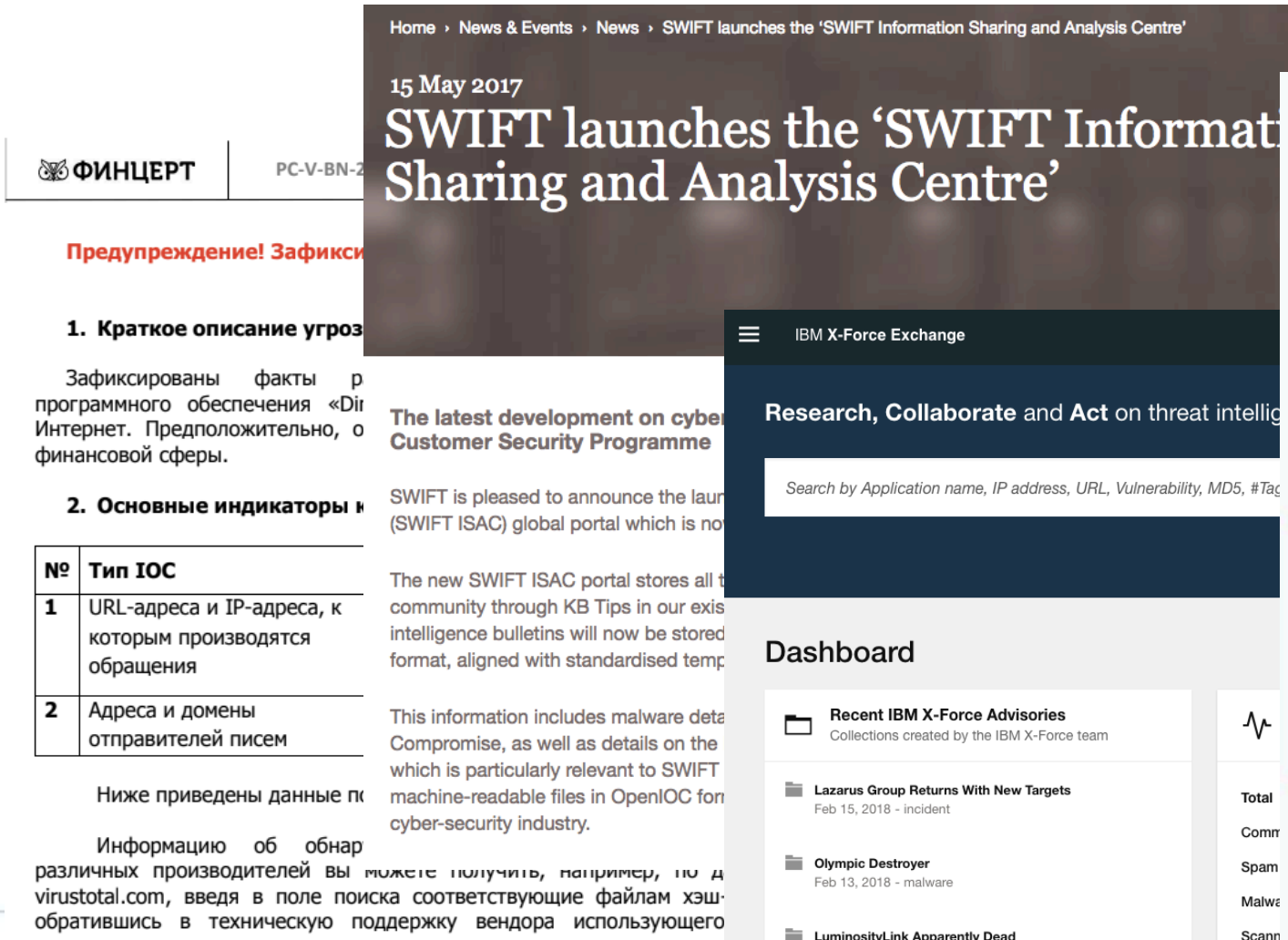
Total	1,165
Command and Control	19
Spam	833
Malware	14
Scanning	303

Vulnerabilities
The latest global security risks

- SAP ERP Financials Information System privilege escalation
  Consequences: Gain Privileges
- SAP Internet Graphics Server (IGS) information disclosure
  Consequences: Obtain Information

Источники данных

ФинЦЕРТ | SWITF | IBM X-Force | AlienVault | Kaspersky …


ФИНЦЕРТ

PC-V-BN-2

Предупреждение! Зафикси

1. Краткое описание угроз

Зафиксированы факты р
программного обеспечения «Dir
Интернет. Предположительно, о
финансовой сферы.

2. Основные индикаторы к

№	Тип IOC
1	URL-адреса и IP-адреса, к которым производятся обращения
2	Адреса и домены отправителей писем

Ниже приведены данные по

Информацию об обнар
различных производителей вы можете получить, например, по д
virustotal.com, введя в поле поиска соответствующие файлам хэш-
обратившись в техническую поддержку вендора использующего

Home › News & Events › News › SWIFT launches the 'SWIFT Information Sharing and Analysis Centre'

15 May 2017

SWIFT launches the 'SWIFT Informati
Sharing and Analysis Centre'

**The latest development on cyber
Customer Security Programme**

SWIFT is pleased to announce the laur
(SWIFT ISAC) global portal which is no

The new SWIFT ISAC portal stores all t
community through KB Tips in our exis
intelligence bulletins will now be stored
format, aligned with standardised temp

This information includes malware deta
Compromise, as well as details on the
which is particularly relevant to SWIFT
machine-readable files in OpenIOC for
cyber-security industry.

IBM X-Force Exchange

Research, Collaborate and Act on threat intellig

Search by Application name, IP address, URL, Vulnerability, MD5, #Tag

Dashboard

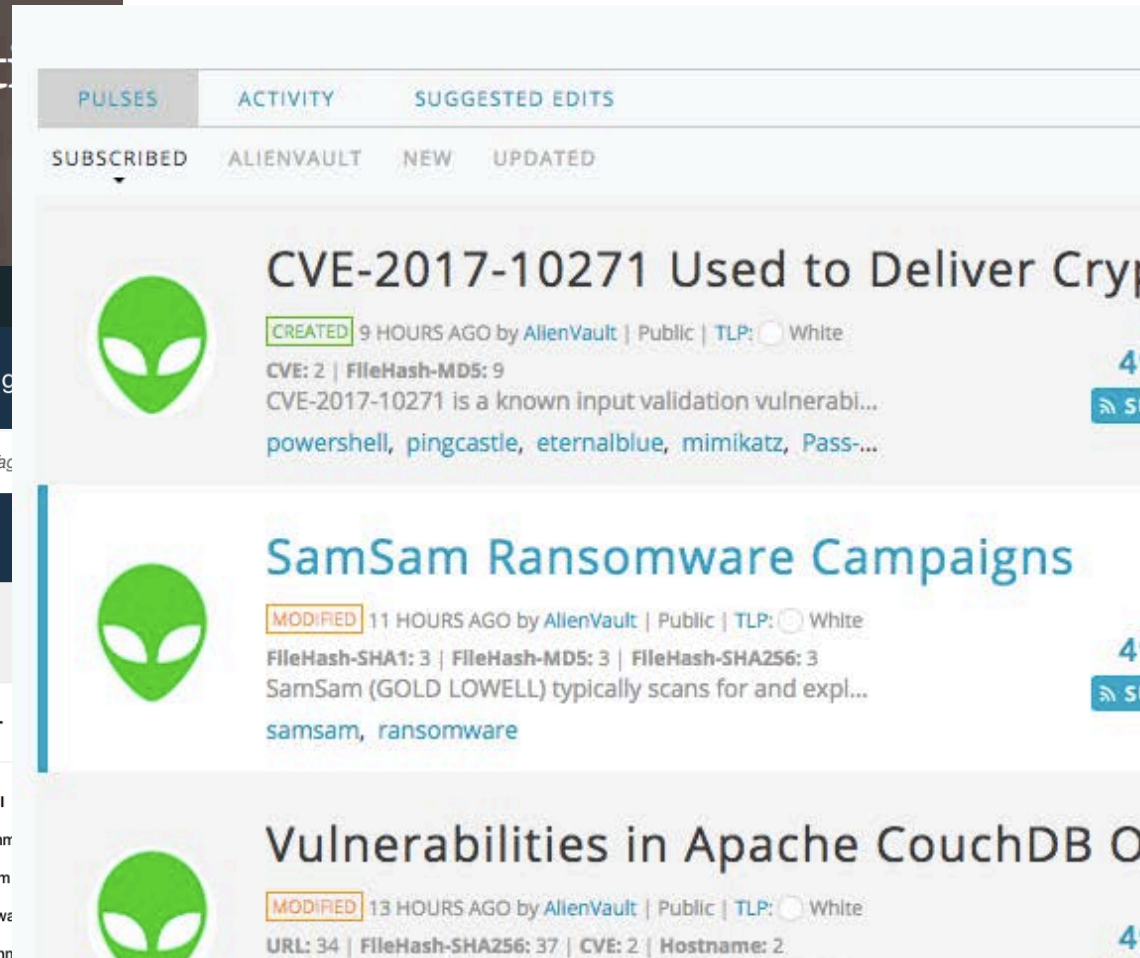
Recent IBM X-Force Advisories
Collections created by the IBM X-Force team

Lazarus Group Returns With New Targets
Feb 15, 2018 - incident

Olympic Destroyer
Feb 13, 2018 - malware

LuminosityLink Apparently Dead

Total
Comm
Spam
Malwa
Scann


PULSES ACTIVITY SUGGESTED EDITS

SUBSCRIBED ALIENVAULT NEW UPDATED

CVE-2017-10271 Used to Deliver Cryp

CREATED 9 HOURS AGO by AlienVault | Public | TLP: White

CVE: 2 | FileHash-MD5: 9

CVE-2017-10271 is a known input validation vulnerabi...

powershell, pingcastle, eternalblue, mimikatz, Pass-...

SamSam Ransomware Campaigns

MODIFIED 11 HOURS AGO by AlienVault | Public | TLP: White

FileHash-SHA1: 3 | FileHash-MD5: 3 | FileHash-SHA256: 3

SamSam (GOLD LOWELL) typically scans for and expl...

samsam, ransomware

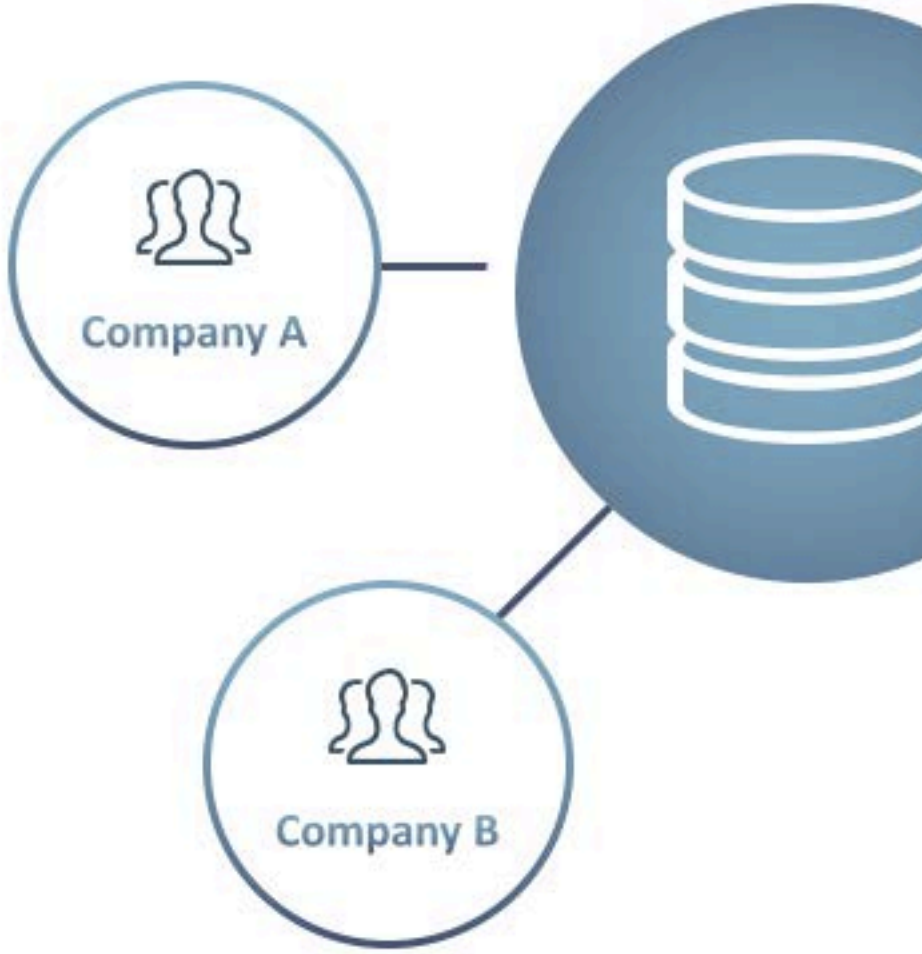
Vulnerabilities in Apache CouchDB O

MODIFIED 13 HOURS AGO by AlienVault | Public | TLP: White

URL: 34 | FileHash-SHA256: 37 | CVE: 2 | Hostname: 2

Механизмы обмена

- Электронная почта
- Файлы
- Программные интерфейсы (API)
- Веб-интерфейсы



Автоматизация реагирования

Поиск по журналам

Проверка конечных узлов

Обновление правил

Мониторинг / блокировка

Ключевые факторы успеха

Ключевые факторы успеха

1

Эффективный инцидент-менеджмент

Ключевые факторы успеха

1 Эффективный инцидент-менеджмент

2 **Централизованный сбор и обработка информации**

Ключевые факторы успеха

1. Эффективный инцидент-менеджмент
2. Централизованный сбор и обработка информации
3. **Техническое решение**


Q
A