

Системы контроля исходящей информации «Перехват»

Версия 2.0

**Скриншоты, описание работы**

(с) ООО «ВВВ Секьюрители»

<http://www-security.com>

<http://perehvat.ru>

## Центр Инцидентов

# Перехват

Copyright 2003-2006 (c) ООО "ВВВ Секьюрити"

<http://perehvat.ru>  
(Q:0 N:0 M:0 F:0 I:0)

[Центр инцидентов](#)

Пользователь: [admin](#) ([Выход](#))

[Системные переменные](#)

Все  Применить фильтр

[Системные пользователи](#)

[Фильтры просмотра](#)

Центр инцидентов (0/4)

[Управление периодами](#)

[Правила автофильтрации](#)

<a href="#">id</a>	<a href="#">period</a>	<a href="#">Источник</a>	<a href="#">Этап</a>	<a href="#">Оценка</a>	<a href="#">robot</a>	<a href="#">Ответственный</a>	<a href="#">Описание</a>	<a href="#">Special</a>
10	1	session	new	unknown	processed		личное письмо	
9	1	session	new	unknown	processed		auth.mail.ru	
8	1	mail	new	violation	processed		письмо про перехват	
7	1	mail	new	unknown	processed		email message	

## Описание

Вся исходящая информация сохраняется и автоматически оформляется в виде инцидентов. На скриншоте показан вид центра инцидентов после автоматической обработки информации (в колонке robot для всех инцидентов стоит значение 'processed') и до начала работы оператора.

Инциденты 7 и 8 (номер инцидента в колонке id) – получились в результате перехвата обычной почты, пересылаемой по протоколу SMTP (см. колонку «Источник»). При автоматической обработке инцидента 8 роботом, сработало правило автофильтрации «перехват», которое выставило описание «письмо про перехват». В соответствии с настройками правил автофильтрации, письма со словом Перехват в теле письма или любого вложения, считаются нарушением. Инцидент автоматически помечен, как нарушение, но этап обработки по прежнему «new». От оператора требуется самостоятельно рассмотреть данные, относящиеся к инциденту, при необходимости провести расследование и выставить свою окончательную оценку. Для инцидента 7 никакие правила не сработали, поэтому его описание стандартное «email message».

Инциденты 9 и 10 получились в результате перехвата веб-трафика (HTTP) на сервер mail.ru. Перехвачена авторизация через сервер auth.mail.ru и само сообщение, которое было отправлено через эту почтовую службу. Через HTTP контролируются не только исходящие сообщения через веб-почту, но и вся остальная исходящая информация, передаваемая через метод POST. В том числе сообщения в форумы, общение на сайтах знакомств, записи в дневники, итд. Для инцидента 10 робот (в соответствии с правилами автофильтрации) выставил описание «личное письмо» (и как будет показано далее, просмотр этого инцидента оператору запрещен).

Через фильтры просмотра (рядом с кнопкой «применить фильтр») оператор может выбрать показ только интересующих его инцидентов. Доступны варианты: «Все», «Все новые», «Все мои» и «Мои в работе».

## Просмотр инцидента

Для просмотра данных любого инцидента достаточно нажать на иконку лупы в правой части таблицы. Для примера, нажмем ее для Инцидента 8.

**Перехват** Copyright 2003-2006 (c) ООО "ВВВ Секьюрити"  
<http://perehvat.ru>  
(Q O H O M O F O I O)

[Центр инцидентов](#) Пользователь: **admin** ([Выход](#))

[Системные переменные](#)

[Системные пользователи](#)

[Фильтры просмотра](#)

[Управление периодами](#)

[Правила автофильтрации](#)

---

**Инцидент #8**

Источник	<a href="#">письмо #2</a>
Этап обработки	new
Оценка	Нарушение
Ответственный	Не назначен
Краткое описание	письмо про перехват
Метки	<b>HAS_DOC</b> <b>perehvat</b> <b>VIOLATION</b>

**Протокол расследования**

Нет записей

По ссылке поля Источник можно перейти на данные о письме, по поводу которого заведена запись инцидента. Этап обработки изначально для всех инцидентов - «new». После того как оператор начинает работу с инцидентом, этап меняется на processing, и по завершении расследования меняется на done. Изначально для данного инцидента роботом выставлена оценка «нарушение», но в ходе работы оператор может изменить ее на ОК если убедится, что фактически нарушения не было. Ответственным за разбор инцидента считается оператор, который ведет работу по нему. Оператор может передать инцидент на расследование другому оператору в зависимости от деталей инцидента (например, всеми нарушениями сотрудников бухгалтерии может заниматься служба безопасности, а для сотрудников IT отдела, начальник IT отдела.). Краткое описание, изначально выставленное роботом, можно изменить по результатам расследования, например, на «Нарушение пункта 3 приказа по фирме о правилах использования сети».

Метки выставляются роботом на основании правил автофильтрации. Метка HAS\_DOC автоматически выставляется если в письме пересылается .doc файл (вложением или внутри архива). Метка perehvat выставляется если в теле письма, или во вложенных документах встречается слово «перехват». Метка VIOLATION выставляется по ряду логических условий, в том числе если есть метка perehvat. Если инцидент имеет метку VIOLATION, робот автоматически выставляет оценку «нарушение».

Ниже ведется протокол расследования. В процессе работы над инцидентом оператор вносит туда записи о ходе расследования. Для каждой записи система хранит время ее создания и имя оператора.

## Приватные инциденты

Copyright 2003-2006 (c) ООО "ВВВ Секьюрити"  
<http://perehvat.ru>  
(Q:0 N:0 M:0 F:0 I:0)

# Перехват

Центр инцидентов Пользователь: [admin](#) ([Выход](#))

[Системные переменные](#) **Инцидент #10**

[Системные пользователи](#) **Инцидент помечен как приватный и запрещен к просмотру**

[Фильтры просмотра](#)

[Управление периодами](#)

[Правила автофильтрации](#)

Существует несколько способов обеспечить защиту части исходящей информации от просмотра операторам. Один из способов – правила автофильтрации, выставляющие метку PRIVATE. Инциденты с меткой PRIVATE недоступны к просмотру.

## Просмотр данных инцидента

Copyright 2003-2006 (c) ООО "ВВВ Секьюрити"  
<http://perehvat.ru>  
(Q:0 N:0 M:0 F:0 I:0)

# Перехват

Центр инцидентов Пользователь: [admin](#) ([Выход](#))

[Системные переменные](#)

[Системные пользователи](#)

[Фильтры просмотра](#)

[Управление периодами](#)

[Правила автофильтрации](#)

recorded	2006-02-09 09:35:50
hfrom	"xx65535yy" <xx65535yy@yandex.ru>
hto	p2demo@perehvat.ru
hsubj	
body	

--  
Яндекс.Почта: объем почтового ящика не ограничен! <http://mail.yandex.ru/monitoring/>

Вложение [FILE ptest.doc](#)

Рассмотрим для примера инцидент 8 (с нарушением – встречается слово «перехват»). Для просмотра данных о сообщении (которые показаны на картинке выше) нужно перейти по ссылке, указанной в графе «источник» на странице инцидента.

Здесь мы видим данные о письме: когда письмо перехвачено, кто отправитель, кто получатель, тему письма, тело и вложения. Слово «перехват», по которому роботом выставлена оценка, не встречается в теле письма. Оно встречается во вложении. Вложение можно скачать и просмотреть кликнув мышкой по ссылке в графе «Вложение».

Если письмо показано в неверной кодировке, нужно ее сменить через меню «Set charset». Чтобы посмотреть все данные о письме («сырой» формат), нужно выбрать «Full» в меню «Field set».

## Вид инцидента после расследования

Перехват

Copyright 2003-2006 (c) ООО "БВВ Секьюрети"  
<http://perehvat.ru>  
 (Q:0 N:0 M:0 F:0 I:0)

[Центр инцидентов](#)
Пользователь: **p2demo** ([Выход](#))

**Инцидент #8**  
 MSG: Статус: done Описание: нарушение п.8

Источник: [письмо #2](#)

Этап обработки:

Оценка:

Ответственный:

Краткое описание:

Метки: **HAS\_DOC**  
**perehvat**  
**VIOLATION**

**Протокол расследования**

admin	2006-02-10 04:55:56
	Ответственный: p2demo Описание: письмо про перехват Статус (auto): processing
p2demo	2006-02-10 04:56:58
	Отправлен запрос нач. службы безопасности о полномочиях отправителя.
p2demo	2006-02-10 04:58:36
	Статус: done Описание: нарушение п.8
p2demo	2006-02-10 04:58:36
	Получен ответ (высылка данных о "перехвате" запрещена). Нарушение п.8 приказа о контроле за информацией. Отчет передан нач. кадровой службы, сотруднику сделан выговор.

Для примера, рассмотрим вариант расследования инцидента номер 8. Пользователь admin, не должен по своим служебным обязанностям разбирать этот инцидент, и он назначает ответственного оператора p2demo, о чем сделана первая запись в протоколе расследования.

Оператор p2demo (в соответствии со своими служебными инструкциями) отправляет запрос начальнику службы безопасности, и по получению ответа от того, передает отчет о расследовании непосредственному начальнику нарушителя, делает соответствующую запись об этом в протоколе расследования меняет описание инцидента и этап обработки на «Done». На этом работа над инцидентом завершена.

Вид центра инцидентов после расследования:

Перехват

Copyright 2003-2006 (c) ООО "БВВ Секьюрети"  
<http://perehvat.ru>  
 (Q:0 N:0 M:0 F:0 I:0)

[Центр инцидентов](#)
Пользователь: **p2demo** ([Выход](#))

Все  Применить фильтр

**Центр инцидентов (0/4)**

id	period	Источник	Этап	Оценка	robot	Ответственный	Описание	Special
10	1	session	new	unknown	processed		личное письмо	
9	1	session	new	unknown	processed		auth.mail.ru	
8	1	mail	done	violation	processed	p2demo	нарушение п.8	
		2006-02-10 04:58:36		Получен ответ (высылка данных о "перехвате" запрещена). Нарушение п.8 приказа о контроле за информацией. Отчет передан нач. кадровой службы, сотруднику сделан выговор.				
7	1	mail	new	unknown	processed		email message	

Пользователь p2demo не является администратором, поэтому ему открыт доступ только в центр инцидентов.

Под каждым завершенным инцидентом или инцидентом в работе пишется последняя запись из протокола расследования, позволяющая быстро видеть прогресс в работе (или его отсутствие).

Каждая запись в протоколе расследования, а так же каждое изменение данных об инциденте (этап, оценка, описание) фиксируются, и в случае если при контрольной проверке инцидентов выясняется, что данные об инциденте не верны (напр. Инцидент с нарушением помечен как нормальный), видно, какой оператор совершил должностное нарушение. Таким образом, за каждое нарушение либо наказывается «нарушитель», либо ответственный оператор, который вел этот инцидент. Ситуация, когда оператор может безнаказанно покрывать нарушения исключена.

## Управление периодами

Перехват

Copyright 2003-2006 (c) ООО "BBB Секьюрити"  
<http://perehvat.ru>  
(Q:O H:O M:O F:O I:O)

[Центр инцидентов](#)  
[Системные переменные](#)  
[Системные пользователи](#)  
[Фильтры просмотра](#)  
[Управление периодами](#)  
[Правила автофильтрации](#)

Пользователь: [admin](#) ([Выход](#))

Текущий период: 1  
Начат: 2006-02-09 09:19:48

При долговременной эксплуатации, имеет смысл разделять время на периоды. В зависимости от объема исходящей информации, новый период может начинаться раз в год или раз в день.

Все новые данные принадлежат к текущему периоду. Одновременно в базе могут находиться данных разных периодов.

Для перехода следует нажать кнопку «Перейти на следующий период». Затем дождаться, когда работа по всем открытые инцидентам будет завершена (день, неделя – в зависимости от объема и сложности работы) и провести архивирование предыдущего периода. При архивировании через браузер будет скачан архив, в котором будут все «сырые» данные и все результаты работы (например, все данные о ходе расследования инцидентов). В дальнейшем архив можно будет обратно загрузить в базу через кнопку «Восстановить из архива».

Если данные какого-либо периода не планируется использовать в ближайшее время и они были помещены в архив, имеет смысл стереть их из базы кнопкой «стереть период».

Важной функцией является возможность пересчитать период. Допустим, в один из предыдущих периодов из сети фирмы «ушла» информация, скажем, о проекте ABC. На тот момент систему еще не сконфигурировали на автоматическое обнаружение этого нарушения. В этом случае правила автофильтрации настраиваются для обработки этого события (например, пометить нарушение при наличии слов «ABC» и «@konkurent.ru» в письме), архив за период, когда вероятно произошло нарушение загружается в систему и отдается команда «пересчитать период». Данные о всех предыдущих метках, инцидентах и расследованиях за этот период стираются из базы и данные обрабатываются заново, что позволяет быстро автоматически найти нарушение.

Благодаря этой функции, потенциальный нарушитель знает, что его нарушение всегда может быть обнаружено, даже если сегодня система не настроена на его автоматическое обнаружение. Контроль за исходящей информацией устанавливается сразу с момента начала перехвата данных, даже если фильтры к тому времени еще не настроены, а политика контроля исходящей информации еще не проработана.

# Правила автоматической фильтрации

## Перехват

Copyright 2003-2006 (c) ООО "ВВВ Секьюрити"  
<http://perehvat.ru>  
(Q:0 N:0 M:0 F:0 I:0)

[Центр инцидентов](#)

Пользователь: [admin](#) (Выход)

[Системные переменные](#)

[Системные пользователи](#)

[Фильтры просмотра](#)

[Управление периодами](#)

[Правила автофильтрации](#)

Table **tagrule** (0/4)

<a href="#">tagname</a>	<a href="#">tagtype</a>	<a href="#">comment</a>	<a href="#">condition</a>	<a href="#">Special</a>
perehvat	text		перехват	
VIOLATION	logic	письмо про перехват	\$perehvat	
PRIVATE	text	личное письмо	личное	
VIOLATION	logic	Архив с паролем	BAD_ARC	

[Add!](#)

Для тестирования и демонстрации в системе заведены следующие правила (показаны на скриншоте):

- Если в сообщении встречается слово «Перехват», инцидент получает метку perehvat
- Все инциденты с меткой perehvat считаются нарушениями
- Все сообщения со словом «личное» помечаются меткой PRIVATE и недоступны операторам.
- Все сообщения с файлами архивов, которые система не может распаковать (т.е. С меткой BAD\_ARC которая выставляется «распаковщиком») и, следовательно, проверить, помечаются как нарушения.

Логические правила могут быть сложнее, включать логические операторы И, ИЛИ, НЕ.

В качестве критериев может так же выступать время отправки, адрес отправителя итд.

Возможна, например, следующая конфигурация:

- Все сообщения с адресов директора фирмы, его заместителей являются приватными.
- Все сообщения от отдела разработки помечаются меткой FROM\_DEV
- Все сообщения на сервер фирмы-партнера помечаются меткой TO\_PARTNER
- Все сообщения о проекте ABC (встречается слово «ABC» или несколько ключевых для проекта слов напр («заказ», «машиностроение», «сверильный станок») помечаются меткой ABC.
- Все сообщения о проекте ABC идущие НЕ между отделом разработки и фирмой-партнером по этому проекту автоматически помечаются как нарушения.