УТВЕРЖДАЮ
Директор ООО «Файнекс»

_____ А.А. Сташевский
20.06.2023

ПОЛОЖЕНИЕ
о мониторинге событий информационной безопасности в ООО «Файнекс»

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о мониторинге событий информационной безопасности в ООО «Файнекс» (далее – Положение) устанавливает цели, задачи, общую организацию мониторинга событий информационной безопасности в ООО «Файнекс» (далее – Организация), а также состав участников процессов мониторинга событий информационной безопасности (далее – мониторинг) и их основные функциональные обязанности.

1.2. Положение разработано в соответствии с Политикой информационной безопасности (кибербезопасности) ООО «Файнекс».

1.3. Для реализации целей и задач мониторинга допускается использование на договорной основе средств, сервисов, персонала и иных ресурсов сторонней (сторонних) организации (-ий).

1.4. Для целей настоящего Положения нижеприведенные термины используются в следующих значениях:

ИБ – информационная безопасность;

объекты мониторинга – компоненты информационной системы Организации, которые осуществляют обработку информационных активов Организации, и (или) реализуют технологические процессы Организации;

источники событий – операционные системы, системы управления базами данных, прикладное программное обеспечение, функционирующие на объектах мониторинга;

событие – сообщение, сгенерированное источником события, зарегистрированное в журнале событий, и поступившее на средства мониторинга;

агент мониторинга – прикладное программное обеспечение, предназначенное для сбора событий от источников событий;

признак инцидента ИБ – сведения, полученные в результате обработки событий, полученных от источника (источников) событий, и свидетельствующие о вероятности наличия инцидента ИБ;

процессы мониторинга – сбор, фильтрация, нормализация, агрегирование, корреляция, приоритезация, категорирование и визуализация событий мониторинга.

1.5. Иные термины, используемые в настоящем Положении, и не

указанные в пункте 1.4 настоящего Положения, имеют значения, определенные нормативными правовыми (техническими нормативными правовыми) актами Республики Беларусь, Наблюдательного совета Администрации Парка высоких технологий, Политикой информационной безопасности (кибербезопасности) ООО «Файнекс».

ГЛАВА 2
ЦЕЛИ, ЗАДАЧИ И ОРГАНИЗАЦИЯ МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Основной целью мониторинга является снижение рисков нарушения ИБ, а также угроз информационным активам и технологическим процессам Организации.

2.2. Задачами мониторинга являются:

организация учета объектов мониторинга;

организация сбора, обработки и анализа событий от объектов мониторинга;

выявление инцидентов (признаков инцидентов) информационной безопасности и проведение их анализа и оценки;

составление по выявленным инцидентам информационной безопасности документов (материалов) и представление их заинтересованным должностным лицам для реализации мер реагирования.

2.3. Для реализации целей и задач мониторинга в Организации создается система мониторинга, включающая:

объекты мониторинга;

субъекты мониторинга;

средства мониторинга;

процессы мониторинга.

2.4. Объектами мониторинга являются:

компоненты информационной системы Организации, реализующие технологические процессы, или осуществляющие обработку информационных активов Организации;

системы (средства) обнаружения вторжений (IDS);

активное сетевое оборудование;

персональные электронно-вычислительные машины работников, включенных в информационную систему Организации.

2.5. Основанием для организации мониторинга объектов является их включение в Реестр объектов мониторинга ООО «Файнекс» (далее – Реестр), составление и сопровождение которого осуществляется системным администратором Организации. Примерная форма Реестра представлена в Приложении 1 к настоящему Положению.

2.6. Мониторинг объектов осуществляется посредством обработки и анализа событий, регистрируемых в журналах безопасности (журналах приложений, системных и иных журналах) источников событий.

На указанные источники разрабатываются правила журналирования событий.

В случае, когда на источниках событий предусмотрено журналирование событий по установленным и неизменяемым правилам, правила журналирования для данных источников не составляются.

2.7. Для реализации целей и задач мониторинга применяются средства мониторинга – программные комплексы (средства), которые реализуют процессы мониторинга событий, поступающих от источников мониторинга.

2.8. В зависимости от технических условий средства мониторинга могут устанавливаться как непосредственно на объекты мониторинга, так и на сервер (серверы) агентов мониторинга.

2.9. Установка средств мониторинга на объекты мониторинга осуществляется системным администратором.

2.10.Для объектов (группы однородных объектов) мониторинга разрабатываются правила корреляции событий источников мониторинга (далее – правила корреляции).

2.11.Об инцидентах ИБ, выявленных в результате мониторинга событий ИБ, проводится информирование заинтересованных должностных лиц, реализуются профилактические мероприятия в соответствии с Планом реагирования на инциденты информационной безопасности.

2.12.Субъектами мониторинга являются работники Организации, выполняющие обязанности в соответствии с Главой 3 настоящего Положения.

ГЛАВА 3
ОБЯЗАННОСТИ РАБОТНИКОВ И ДОЛЖНОСТНЫХ ЛИЦ ПО ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЮ СИСТЕМЫ МОНИТОРИНГА

3.1. Системный администратор:

вырабатывает предложения по целям, задачам и организации мониторинга событий ИБ;

составляет и актуализирует Реестр;

разрабатывает правила журналирования источников событий;

разрабатывает и тестирует правила корреляции событий (организует на договорной основе разработку правил корреляции сторонней организацией);

разрабатывает План реагирования на инциденты ИБ;

вырабатывает предложения по приобретению и использованию средств мониторинга;

осуществляет эксплуатацию средств мониторинга;

обеспечивает реализацию процессов мониторинга;

выявляет инциденты ИБ, проводит по ним разбирательства и реализует профилактические меры.

Приложение 1
к Положению о мониторинге событий
информационной безопасности
в ООО «Файнекс»

Примерная форма

РЕЕСТР ОБЪЕКТОВ МОНИТОРИНГА ООО «ФАЙНЕКС»

N п\п	Сетевое имя объекта мониторинга	IP-адрес	Тип объекта мониторинга[1]	Характеристика источника событий мониторинга[2]	Категории обрабатываемой информации[3]	Функция объекта мониторинга

[1] Сервер БД, прокси-сервер, межсетевой экран, IDS, рабочая станция и т.д.

[2] ОС Windows, Oracle и т.д.

[3] Банковская тайна, коммерческая тайна, служебная информация ограниченного распространения, персональные данные