УТВЕРЖДАЮ
Директор ООО «Файнекс»

_____А.А. Сташевский
20.06.2023

ПОЛОЖЕНИЕ
об управлении уязвимостями компонентов информационной системы ООО «Файнекс»

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об управлении уязвимостями компонентов информационной системы ООО «Файнекс» (далее – Положение) определяет цели, задачи, организацию процесса управления уязвимостями компонентов информационной системы ООО «Файнекс» (далее – Организация), а также функциональные обязанности структурных подразделений Организации, участвующих в данном процессе.

1.2. В настоящем Положении нижеприведенные термины имеют следующие определения:

ИБ – информационная безопасность;

ПО – программное обеспечение;

компенсационные меры – организационные и (или) практические меры, которые могут использоваться Организацией для снижения рисков нарушения ИБ до требуемого уровня в случае объективной невозможности выполнения требований технических нормативных правовых актов регуляторов; компенсационные меры должны удовлетворять требованиям регуляторов;

компоненты информационной системы Организации – серверное оборудование, активное сетевое оборудование, средства обеспечения безопасности, персональные компьютеры;

уязвимость – слабое место (недостаток) в информационной системе Организации, которое может быть использовано нарушителем для реализации угрозы ИБ. Уязвимость может быть результатом ошибок в системном, прикладном, микропрограммном ПО, недостатков, допущенных при проектировании и (или) эксплуатации информационной системы Организации;

сканер уязвимостей – средство обнаружения уязвимостей в ПО компонентов информационной системы Организации;

управление уязвимостями – действия, направленные на обнаружение и классификацию уязвимостей, а также на их устранение или снижение рисков их эксплуатации;

эксплойт – компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в ПО и применяемые для проведения атаки на информационную систему Организации. Целью атаки может

быть как захват контроля над системой (повышение привилегий), так и нарушение ее функционирования;

CVSS (Common Vulnerability Scoring System) - общая система оценки уязвимостей;

OWASP (Open Web Application Security Project) – открытый (некоммерческий) проект по безопасности веб-приложений;

CWE (Common Weakness Enumeration) – перечень известных уязвимых мест ПО (исходного кода);

OSSTMM (Open Source Security Testing Methodology Manual) – открытое руководство по методологии тестирования безопасности ПО (исходного кода).

1.3. Иные термины, используемые в настоящем Положении, и не указанные в пункте 2, имеют значения, определенные нормативными правовыми (техническими нормативными правовыми) актами Республики Беларусь, актами Наблюдательного совета Парка высоких технологий, Политикой информационной безопасности (кибербезопасности) ООО «Файнекс».

ГЛАВА 2
ЦЕЛИ, ЗАДАЧИ И ОРГАНИЗАЦИЯ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

2.1. Целью процесса управления уязвимостями является повышение уровня ИБ компонентов информационной системы и информационных активов Организации.

2.2. Задачами процесса управления уязвимостями являются:

планирование и реализация мероприятий по выявлению и оценке уязвимостей компонентов информационной системы Организации (далее – Мероприятия);

документирование результатов Мероприятий;

доведение результатов Мероприятий до заинтересованных работников Организации;

реализация выводов и предложений по результатам Мероприятий.

2.3. Мероприятиями по выявлению и оценке уязвимостей компонентов информационной системы Организации являются:

мониторинг внешних источников информации об уязвимостях и установка обновлений безопасности, выпущенных поставщиком ПО;

внутренние сканирования на наличие уязвимостей;

внешние сканирования на наличие уязвимостей;

внутренние тесты на проникновение;

внешние тесты на проникновение;

проверка защищенности веб-приложений.

2.4. Для проведения Мероприятий в Организации составляется план мероприятий по оценке защищенности компонентов информационной системы Организации по примерной форме, представленной в Приложении 1 к настоящему Положению (далее – План мероприятий).

План мероприятий составляется на календарный год системным администратором и утверждается директором Организации.

2.5. Для проведения Мероприятий Организацией могут привлекаться

сторонние организации. В таком случае в договоры на производство работ и услуг должны быть включены требования:

по обеспечению конфиденциальности информации. Указанные требования могут быть оформлены в виде соглашения о конфиденциальности;

о недопустимости действий, которые могут привести к уничтожению информации или нарушению работоспособности компонентов информационной системы Организации, такие, например, как атаки на отказ в обслуживании;

о прекращении исполнителем работ до получения от Организации формального разрешения на продолжение работ в случаях высокой вероятности нарушения функционирования информационной системы Организации (ее компонентов) или в случаях успешного доступа к конфиденциальной информации Организации.

2.6. Выявленные в процессе проведения Мероприятий уязвимости и риски, обусловленные данными уязвимостями, обрабатываются в соответствии с локальными правовыми актами Организации, регламентирующими процессы управления рисками нарушения информационной безопасности.

ГЛАВА 3
ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ С ПОМОЩЬЮ АВТОРИТЕТНЫХ ВНЕШНИХ ИСТОЧНИКОВ ИНФОРМАЦИИ И УСТАНОВКА ОБНОВЛЕНИЙ БЕЗОПАСНОСТИ, ВЫПУЩЕННЫХ ПОСТАВЩИКОМ ПО

3.1. Для своевременного получения информации о новых уязвимостях, которые могут оказать влияние на среду обработки информационных активов Организации, а также превентивной защиты компонентов информационной системы Организации, осуществляется мониторинг авторитетных источников информации об уязвимостях и установка обновлений безопасности, выпущенных поставщиком ПО.

3.2. В качестве достоверных источников информации об уязвимостях могут быть:

веб-сайты поставщиков ПО;

веб-сайты специализированных учреждений по ИБ;

отраслевые новостные группы, почтовые рассылки или RSS-потоки.

3.3. Мониторинг источников информации об уязвимостях осуществляется системным администратором Организации.

3.4. После выявления новой уязвимости определяется риск, который обусловлен данной уязвимостью.

Оценка риска осуществляется с учетом среды проявления, потенциального влияния на целостность, конфиденциальность и доступность информационных активов Организации, возможных потерь для нее и иных обстоятельств в соответствии с локальными правовыми актами Организации, регламентирующими процессы управления рисками нарушения информационной безопасности.

3.5. Для устранения уязвимостей системным администратором Организации устанавливаются обновления безопасности, выпущенные поставщиками (разработчиками) ПО.

3.6. Перед установкой обновлений безопасности осуществляется проверка

их функциональности с целью убедиться в том, что внесенные изменения не оказывают неблагоприятного воздействия на работоспособность информационной системы Организации или ее компонентов.

Тестирование обновлений осуществляется в тестовой среде. В качестве тестовой среды могут использоваться компоненты информационной системы Организации, на которых не реализуются критичные технологические (информационные) процессы Организации.

3.7. На компоненты информационной системы Организации, реализующие платежные технологические процессы, обновления безопасности для уязвимостей с уровнем риска «критичный» устанавливаются в срок, как правило, не превышающий одного календарного месяца с момента выпуска данного обновления поставщиком ПО, для уязвимостей с меньшим уровнем риска, как правило, – в срок не более трех месяцев с момента выпуска данного обновления поставщиком ПО.

3.8. На компоненты информационной системы Организации, реализующие информационные технологические процессы, обновления безопасности для уязвимостей с уровнем риска «критичный» устанавливаются в срок, как правило, не превышающий трех месяцев с момента выпуска данного обновления поставщиком ПО, для уязвимостей с меньшим уровнем риска, как правило, – в срок не более шести месяцев с момента выпуска данного обновления поставщиком ПО.

3.9. Как правило, обновления ПО осуществляются в рамках запланированных регламентных или иных работ.

3.10.Тестирование и установку обновлений безопасности осуществляет системный администратор Организации.

К проведению работ по тестированию и установке обновлений безопасности могут привлекаться иные заинтересованные работники Организации и (или) сторонних организаций.

ГЛАВА 4
ОСОБЕННОСТИ ПРОВЕДЕНИЯ ВНУТРЕННИХ СКАНИРОВАНИЙ

4.1. Внутренние сканирования проводятся внутри информационной системы Организации с целью выявления и устранения уязвимостей ее компонентов.

4.2. Внутренние сканирования проводятся системным администратором в отношении:

компонентов информационной системы Организации – в соответствии с Планом мероприятий;

сегментов информационной системы Организации после внесения в них значительных изменений – по факту внесения изменений;

компонентов, предполагаемых к включению в информационную систему Организации, – в тестовой среде или выделенном сегменте локальной вычислительной сети до включения в производственную среду.

4.3. Для организации внутреннего сканирования системным администратором составляется план проведения внутреннего сканирования по примерной форме согласно Приложению 2 к настоящему Положению.

4.4. По результатам сканирования системным администратором формируется отчет, в котором указываются: IP-адреса отсканированных компонентов информационной системы Организации, обнаруженные уязвимости; уровень их критичности; описание уязвимости; рекомендации по устранению уязвимости.

4.5. На стадии подготовки отчета по результатам внутреннего сканирования в рабочем порядке выявляются возможные ложные срабатывания сканера уязвимостей, а также анализируются возможность и сроки устранения (снижения критичности) уязвимостей или применения компенсационных мер для снижения рисков нарушения ИБ.

4.6. В отношении компонентов информационной системы Организации, на которых были реализованы меры по устранению (снижению критичности) уязвимостей, проводится повторное сканирование.

4.7. Для отчетности допускается объединение нескольких отчетов сканера о результатах сканирования для подтверждения того, что все системы были просканированы, а все найденные уязвимости – устранены.

ГЛАВА 5
ОСОБЕННОСТИ ПРОВЕДЕНИЯ ВНЕШНИХ СКАНИРОВАНИЙ

5.1. Внешние сканирования проводятся в отношении систем и сервисов, доступных из сети Интернет, для обнаружения потенциальных уязвимостей, которые могут быть использованы злоумышленниками.

5.2. Внешние сканирования проводятся в соответствии с Планом мероприятий, а также после внесения изменений в состав и ПО компонентов информационной системы Организации, доступных из сети Интернет.

5.3. Процедура внешнего сканирования предусматривает повторные сканирования до тех пор, пока не будут устранены уязвимости со степенью критичности 4.0 или выше по шкале CVSS.

ГЛАВА 6
ОСОБЕННОСТИ ПРОВЕДЕНИЯ ВНЕШНЕГО ТЕСТА НА ПРОНИКНОВЕНИЕ

6.1. Целью выполнения внешнего теста на проникновение (далее – внешний тест) является повышение уровня защищенности информационной системы Организации от атак, которые могут быть реализованы из сети Интернет через сетевой периметр информационной системы Организации.

6.2. В рамках внешнего теста реализуются следующие задачи:

имитация атак из сети Интернет, которые могут реализовать реальные злоумышленники для получения несанкционированного доступа к компонентам информационной системы Организации, веб-приложениям и информационным активам Организации;

выявление уязвимостей компонентов информационной системы Организации, определение возможности применения эксплойтов;

получение логического доступа к компонентам информационной системы Организации;

получение доступа к информационным активам, обрабатываемым в информационной системе Организации;

выявление возможности совершения мошеннических действий в информационной системе Организации;

определение возможности нарушения работоспособности компонентов информационной системы Организации путем нарушения целостности обрабатываемых данных или нарушения доступности функционирующих сервисов;

анализ защищенности информационной системы Организации;

разработка рекомендаций по повышению уровня защищенности информационной системы Организации и снижения рисков нарушения ИБ.

6.3. Объектами внешних тестов являются компоненты информационной системы Организации, размещенные на периметре корпоративной сети и доступные из сети Интернет.

В случае успешной реализации атаки на указанные компоненты, в границы работ по внешнему тестированию на проникновение могут входить ставшие доступными серверное и сетевое оборудование, персональные компьютеры, средства безопасности информационной системы Организации.

6.4. Внешние тесты проводятся не реже одного раза в год, а также после любой значительной модификации или обновления ИТ-инфраструктуры, системного или прикладного ПО (например, обновления операционной системы, изменения топологии локальной вычислительной сети, установки веб-сервера, активных средств сетевой безопасности).

6.5. Внешние тесты проводятся работниками сторонней организации, организационно не зависящей от Организации.

6.6. Внешние тесты проводятся по методике исполнителя с использованием методов сбора данных, идентификации и эксплуатации уязвимостей, а также получения доступа к информационным системам, на основе требований и рекомендаций различных международных стандартов (методик), таких как OWASP, OSSTMM и др.

При этом анализ включает как минимум проверку на наличие уязвимостей, таких как OWASP Top-10, CWE Top-25.

6.7. По результатам внешнего теста исполнитель представляет отчет с результатами проведенных проверок.

ГЛАВА 7
ОСОБЕННОСТИ ПРОВЕДЕНИЯ ВНУТРЕННЕГО ТЕСТА НА ПРОНИКНОВЕНИЕ

7.1. Целью выполнения внутреннего теста на проникновение (далее – внутренний тест) является повышение уровня защищенности информационной системы Организации от атак, которые могут быть реализованы из корпоративной сети Организации.

7.2. В рамках внутреннего теста реализуются следующие задачи:

имитация атак из корпоративной сети Организации, которые могут реализовать реальные злоумышленники для получения несанкционированного доступа к информационным активам Организации;

выявление уязвимостей компонентов информационной системы Организации, определение возможности применения эксплойтов;

получение логического доступа к компонентам информационной системы Организации;

получение доступа к информационным активам, обрабатываемым в информационной системе Организации;

выявление возможности совершения мошеннических действий в информационной системе Организации;

определение возможности нарушения работоспособности компонентов информационной системы Организации путем нарушения целостности обрабатываемых данных или нарушения доступности функционирующих сервисов;

анализ защищенности информационной системы Организации;

разработка рекомендаций по повышению уровня защищенности информационной системы Организации и снижения рисков нарушения ИБ.

7.3. Работы проводятся по методике исполнителя с использованием методов сбора данных, идентификации и эксплуатации уязвимостей, а также получения доступа к информационным системам и ресурсам, на основе требований и рекомендаций различных международных стандартов и лучших практик в области ИБ, а также различных методик оценки защищенности.

В набор использованных методов не должны входить способы намеренного уничтожения данных или нарушения работоспособности устройств, такие как атаки на отказ в обслуживании.

7.4. В рамках работ по внутреннему тестированию реализуется модель действий злоумышленника, имеющего возможность подключения к информационной системе Организации, но не имеющего логических прав в информационной системе Организации и не обладающего сведениями о ее составе.

В рамках указанной модели специалисту, имитирующему потенциального злоумышленника (далее – тестировщик), предоставляется ПЭВМ, подключенная к пользовательскому сегменту локальной вычислительной сети Организации, с установленным на ней стандартным (определенным для рабочих мест) системным и прикладным ПО.

7.5. Со стороны Организации осуществляется:

координация процесса тестирования и действий тестировщика;

контроль имеющимися средствами обеспечения ИБ за деятельностью тестировщика в информационной системе Организации;

регистрация событий, генерируемых компонентами информационной системы Организации в качестве реакции на попытки проникновения, получения логического доступа, использования эксплойтов и иных действий в процессе тестирования;

предоставление тестировщику для включения в отчет о тестировании документированных подтверждений о контроле процесса тестирования и об этапах тестирования, на которых могли быть локализованы и (или) предотвращены атаки.

7.6. Внутренний тест проводится не реже одного раза в год, а также после любой значительной модификации или обновления инфраструктуры и ПО в

информационной системе Организации.

7.7. Внутренний тест проводится работниками сторонней организации, организационно не зависящей от Организации.

7.8. По результатам внутреннего теста исполнитель представляет отчет с результатами проведенных проверок.

ГЛАВА 8
ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ РАБОТНИКОВ ОРГАНИЗАЦИИ, УЧАСТВУЮЩИХ В ПРОЦЕССЕ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

8.1. Системный администратор или должностное лицо, ответственное за системное администрирование и информационную безопасность в Организации):

вырабатывает предложения по целям, задачам и способам реализации процесса управления уязвимостями компонентов информационной системы Организации;

составляет Планы мероприятий;

осуществляет мониторинг уязвимостей с помощью авторитетных внешних источников информации об уязвимостях;

осуществляет проведение Мероприятий в соответствии с Планом мероприятий, составляет отчеты и направляет их для исполнения заинтересованным работникам Организации;

осуществляет контроль устранения уязвимостей или реализации в отношении данных уязвимостей компенсирующих мер.

устанавливает обновления безопасности системного и прикладного ПО;

реализует Мероприятия по устранению уязвимостей или реализации компенсирующих мер.

Приложение 1
к Положению по управлению уязвимостями информационной системы ООО «Файнекс»

Примерная форма

ПЛАН
мероприятий по оценке защищенности компонентов информационной системы ООО «Файнекс»

№ п/п	Наименование мероприятия	Срок проведения мероприятия	Структурное подразделение, ответственное за проведение мероприятия	Отметка о проведении мероприятия	Примечание

(наименование должности) (подпись) (И.О.Фамилия)

Приложение 2
к Положению по управлению уязвимостями информационной системы ООО «Файнекс»

Примерная форма

ПЛАН
проведения внутреннего сканирования на наличие уязвимостей компонентов информационной системы ООО «Файнекс»

Дата начала проведения сканирования	
Основание для проведения сканирования	
IP-адрес компьютера, с которого производится сканирование	
Диапазон (диапазоны) IP-адресов узлов, подлежащих сканированию	
Наименование и версия используемого сканера уязвимостей	
Диапазоны TCP/UDP сканируемых портов	
Используемые политики сканирования на уязвимости	
Фамилия и инициалы, контактные телефоны лиц, проводящих сканирование	

_____ _____ _____
(наименование должности) (подпись) (И.О.Фамилия)

_____
(дата)