ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ГЕОДЕЗИИ И КАРТОГРАФИИ

Отчет по заданию ФСТЭК

Вариант 8

|  |
| --- |
| Выполнила:  Студентка 2021-ФГиИБ-ИБ-1б  Басова Мария Вячеславовна |

Москва 2023

**Роли пользователей в системе Flatpress:**

1. **Пользователь:**

Этот уровень доступа обычно позволяет только комментировать посты и страницы блога. Пользователи могут оставлять комментарии, но не могут создавать или редактировать контент. Могут подписываться на обновления блога, получая уведомления о новых записях.

1. **Администратор информационной системы (Админ ИС):**

Ответственные за общее управление и настройку самой системы Flatpress.

* + - Обновление Flatpress.
    - Управление пользователями и их ролями.
    - Мониторинг производительности и общего состояния системы.
    - Резервное копирование данных.
    - Управление темами и плагинами.

1. **Администратор информационной безопасности (Админ ИБ):**

Занимается обеспечением безопасности системы и данных в Flatpress.

* + - Настройка и мониторинг системы безопасности.
    - Реагирование на инциденты безопасности и расследование инцидентов.
    - Обеспечение соответствия системы нормативам и стандартам безопасности.
    - Управление аутентификацией и авторизацией.
    - Обеспечение безопасности передачи данных, включая протоколы шифрования.

**Опросник негативных последствий:**

|  |  |  |
| --- | --- | --- |
| **Виды риска (ущерба) и возможные негативные последствия** | **Виды актуального нарушителя** | **Уровень возможностей нарушителя** |
| |  | | --- | | У1: нарушение конфиденциальности персональных данных граждан; нарушение личной, семейной тайны, утрата чести и доброго имени; финансовый, иной материальный ущерб физических лиц | | | |  | | --- | | Преступные группы (криминальные структуры) | | Отдельные физические лица (хакеры) | | Разработчики программных, программно-аппаратных средств | | Системные администраторы и администраторы безопасности | | Авторизованные пользователи систем и сетей | | Преступные группы (криминальные структуры) | | Отдельные физические лица (хакеры) | | |  | | --- | | Н3 | | Н2 | | Н2 | | Н2 | | Н2 | | Н2 | | Н1 | |
| У2: невозможность заключения договоров, соглашений; утечка коммерческой тайны; потеря клиентов; нарушение деловой репутации; недополучение ожидаемой прибыли | |  | | --- | | Разработчики программных, программно-аппаратных средств | | Системные администраторы и администраторы безопасности | | Специальные службы иностранных государств | | Террористические, экстремистские организации | | Преступные группы (криминальные структуры) | | |  | | --- | | Н4 | | Н2 | | Н4 | | Н3 | | Н2 | |
| У3: нарушение функционирования государственного органа, дискредитация деятельности органа государственной власти; доступ к системам и сетям с целью незаконного использования вычислительных мощностей; утечка информации ограниченного доступа; организация митингов, забастовок из-за публикаций недостоверной информации; отсутствие доступа к социально значимым государственным услугам | |  | | --- | | Разработчики программных, программно-аппаратных средств | | Системные администраторы и администраторы безопасности | | Авторизованные пользователи систем и сетей | | Бывшие (уволенные) работники (пользователи) | | |  | | --- | | Н4 | | Н3 | | Н2 | | Н2 | |

**Уровни возможностей нарушителя:**

Н1 - Нарушитель, обладающий базовыми возможностями.

* Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети "Интернет"
* Физическое лицо (хакер); лица, работающие в этой организации и имеющие доступ в помещения (администрация, охрана, уборщики и т.д.); авторизованные пользователи; бывшие работники.

Н2 - Нарушитель, обладающий базовыми повышенными возможностями.

* Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети "Интернет" и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз.  Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении.
* Преступные группы (два лица и более, действующие по единому плану); конкурирующие организации; поставщики вычислительных услуг; лица, привлекаемые для установки, настройки, испытаний и иных видов работ; системные администраторы и администраторы безопасности (как работающие, так и уволенные)

Н3 - Нарушитель, обладающий средними возможностями.

* Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств.
* Террористические, экстремистские группировки; разработчики программных, программно-аппаратных средств; преступные группы, в состав которых входят бывшие и действующие работники (администраторы).

Н4 - Нарушитель, обладающий высокими возможностями.

* Обладает всеми возможностями нарушителей со средними возможностями. Имеет возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях "нулевого дня". Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств. Имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и специально разработанных средств.
* Специальные службы иностранных государств, запрещённые группировки.

**Объяснение опросника НП:**

**У1:**

1. Преступные группы (криминальные структуры):

*Уровень возможностей нарушителя:* Высокий (Н3)

* Эти лица могут иметь высокий уровень организации, ресурсов и технических навыков для проведения сложных атак, включая взломы, кражи данных и их последующее использование в мошеннических схемах.

1. Отдельные физические лица (хакеры):

*Уровень возможностей нарушителя:* Средний, но немного высокий (Н2)

* Опытные хакеры среднего и высокого уровня могут использовать различные методы атак, такие как эксплойты, социальная инженерия и вредоносные программы для доступа к персональным данным и их злоупотребления.

1. Разработчики программных, программно-аппаратных средств:

*Уровень возможностей нарушителя:* Средний (Н2)

* Разработчики могут исследовать уязвимости и создавать специализированные инструменты для атак, но их возможности обычно ограничены эксплуатацией известных уязвимостей.

1. Системные администраторы и администраторы безопасности:

*Уровень возможностей нарушителя:* Средний (Н2)

* Администраторы могут злоупотреблять своими привилегиями, но их действия ограничены политиками безопасности.

1. Авторизованные пользователи систем и сетей:

*Уровень возможностей нарушителя:* Низкий (Н1)

* Пользователи с ограниченными правами имеют меньше возможностей для проведения масштабных атак; однако возможны утечки данных.

**У2:**

1. Разработчики программных, программно-аппаратных средств:

*Уровень возможностей нарушителя:* Высокий (Н4)

* Эти лица имеют доступ к исходному коду системы и могут внести недокументированные изменения, создавая уязвимости и открывая доступ к конфиденциальной информации.

1. Системные администраторы и администраторы безопасности:

*Уровень возможностей нарушителя:* Средний (Н2)

* Администраторы имеют прямой доступ к серверам и системам, что может сделать их способными изменять настройки, собирать информацию и организовывать утечки данных, но ограничены политиками безопасности.

1. Специальные службы иностранных государств:

*Уровень возможностей нарушителя:* Высокий (Н4)

* Данные службы обладают высокими ресурсами, техническими возможностями и разнообразными методами для проведения кибератаки на информационные системы.

1. Террористические, экстремистские организации:

*Уровень возможностей нарушителя:* Средний (Н2)

* Эти организации могут внедряться в систему и использовать ее для своих целей, однако вряд ли у них есть высокие технические навыки.

1. Преступные группы (криминальные структуры):

*Уровень возможностей нарушителя:* Высокий (Н3)

* Преступные группы зачастую имеют широкий спектр ресурсов и специалистов, включая хакеров, способных осуществлять целенаправленные атаки для получения коммерческой тайны и другой ценной информации.

**У3:**

1. Разработчики программных, программно-аппаратных средств:

*Уровень возможностей нарушителя:* Высокий (Н3)

* Разработчики программных и программно-аппаратных средств имеют высокий уровень знаний и навыков, необходимых для нарушения безопасности системы. Они могут создавать и внедрять вредоносные программы, взламывать системные уязвимости и проводить другие атаки, целью которых является нарушение функционирования государственного органа, дискредитация его деятельности или утечка ограниченной информации.

1. Системные администраторы и администраторы безопасности:

*Уровень возможностей нарушителя:* Высокий (Н3)

* Системные администраторы и администраторы безопасности обладают знаниями и привилегиями, позволяющими им получить доступ к системам и сетям. Они могут организовать незаконное использование вычислительных мощностей, утечку информации или нарушение доступа к государственным услугам. Однако, их возможности могут быть ограничены законодательством и внутренними правилами организации.

1. Авторизованные пользователи систем и сетей:

*Уровень возможностей нарушителя:* Средний (Н1)

* Авторизованные пользователи систем и сетей могут осуществлять действия, которые противоречат интересам государственного органа. Они могут публиковать недостоверную информацию, организовывать митинги и забастовки, но их возможности ограничены уровнем доступа и правами, которые им предоставлены.

1. Бывшие (уволенные) работники (пользователи):

*Уровень возможностей нарушителя:* Средний (Н2)

* Бывшие работники, которые имели доступ к системе и сети, всё ещё могут иметь некоторые возможности для нарушения безопасности. Однако, эти возможности будут ограничены после увольнения и могут быть связаны только с ограниченным доступом к информации или возможностью распространения недостоверных данных.

|  |  |  |  |
| --- | --- | --- | --- |
| Номер УБИ | Наименование УБИ | Категория нарушителя и его возможности | Какое свойство информации нарушает |
| УБИ.002 | Угроза несанкционированного доступа к системным данным | Внешний нарушитель с высоким потенциалом,  Внутренний нарушитель с высоким потенциалом. | Конфиденциальность |
| УБИ.005 | Угроза повреждения информации | Внешний нарушитель с высоким потенциалом,  Внутренний нарушитель с высоким потенциалом. | Целостность |
| [УБИ.008](https://service.securitm.ru/bdu/threat/ubi-8) | Угроза нарушения функционирования (работоспособности) | Внешний нарушитель с высоким потенциалом,  Внутренний нарушитель с высоким потенциалом. | Доступность и Целостность |
| УБИ.010 | Угроза несанкционированного удаления защищаемой информации | Внешний нарушитель с высоким потенциалом,  Внутренний нарушитель с высоким потенциалом. | Конфиденциальность и Целостность |
| УБИ.027 | Угроза искажения вводимой и выводимой на периферийные устройства информации | Внешний нарушитель с низким потенциалом;  Внутренний нарушитель с низким потенциалом. | Целостность |
| УБИ. 088 | Угроза несанкционированного копирования защищаемой информации | Внешний нарушитель с низким потенциалом;  Внутренний нарушитель с низким потенциалом | Конфиденциальность |
| УБИ.111 | Угроза передачи данных по скрытым каналам | Внешний нарушитель с высоким потенциалом | Целостность |
| УБИ.140 | Угроза приведения системы в состояние "отказ в обслуживании" | Внешний.  Отказ в обслуживании (DoS) | Доступность |
| УБИ.122  УБИ.031 | Злоумышленное использование привилегий | Внутренний нарушитель с высоким потенциалом. | Конфиденциальность |
| УБИ.208. | Угроза нецелевого использования вычислительных ресурсов | Внутренний нарушитель с низким потенциалом | Доступность |