Министерство образования
Республики Беларусь

Учреждение образование
«Гомельский государственный
Университет имени Франциска
Скорины»

УТВЕРЖДАЮ

Ректор учреждения образования
«Гомельский государственный
университет имени Франциска
Скорины»

_____ С.А.Хахомов

_____ 2024

ИНСТРУКЦИЯ
24.05.2024 № И-2/23
г. Гомель

о порядке действий работников и обучающихся университета при реагировании на инциденты информационной безопасности

1. Общие положения

1.1. Настоящая Инструкция «О порядке действий работников и обучающихся университета при реагировании на инциденты информационной безопасности» (далее – Инструкция) определяет порядок действий работников и обучающихся Учреждения образования «Гомельский государственный университет имени Франциска Скорины» (далее – Университет) при реагировании на инциденты информационной безопасности.

1.2. В настоящей Инструкции используются следующие термины и определения:

1.2.1. Инцидент информационной безопасности (далее – ИБ) - непредвиденное или нежелательное событие (группа событий) ИБ, которое привело (могут привести) к нарушению функционирования информационного ресурса или возникновению угроз безопасности информации, или нарушению требований по защите информации.

1.2.2. Внутренний инцидент ИБ – инцидент, источником которого является нарушитель, связанный с пострадавшей стороной (Университетом) непосредственным образом (трудовым договором или иным способом).

1.2.3. Внешний инцидент ИБ – инцидент, источником которого является нарушитель, не связанный с пострадавшей стороной (Университетом) непосредственным образом.

1.2.4. Обучающийся – лицо, зачисленное в Университет для освоения содержания образовательной программы, реализуемой Университетом.

1.2.5. Инциденты ИБ разделяют:
по типам (или видам),
по степени критичности (или степени возможно ущерба) для организации.

1.3. Виды инцидентов ИБ:

1.3.1. утечка конфиденциальной информации;

1.3.2. неправомерный доступ к информации;

1.3.3. удаление (скрытое шифрование) информации;

1.3.4. компрометация информации;

1.3.5. саботаж;

1.3.6.мошенничество посредством информационно-коммуникационных технологий (далее – ИКТ);

1.3.7. аномальная сетевая активность;

1.3.8.использование активов Университета в личных целях или в мошеннических операциях.

1.4. По типу можно выделить следующие инциденты ИБ:

1.4.1. Киберинциденты высокого уровня (далее – КВУ):

внедрение и функционирование вредоносных программ на объектах информационной инфраструктуры (далее – ИИ);

несанкционированный доступ к объектам ИИ с использованием ИКТ;

использование объектов ИИ для осуществления кибератак и (или) распространения вредоносных программ;

прослушивание, захват, перенаправление сетевого трафика объектов ИИ;

рассылка незапрашиваемой информации (спама) с объектов ИИ;

эксплуатация уязвимостей на объектах ИИ;

прекращение функционирования объектов ИИ, вызванное кибератакой типа «отказ в обслуживании».

1.4.2. Киберинциденты низкого уровня (далее – КНУ):

попытка внедрения вредоносных программ на объектах ИИ;

атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS), направленной на объекты ИИ, не вызвавшей негативных последствий;

попытка эксплуатации уязвимостей на объектах ИИ;

сканирование объектов ИИ в целях поиска уязвимостей;

попытка несанкционированного доступа к объектам ИИ;

прекращение функционирования объектов ИИ, не связанное с КВУ;

попытка использования объектов ИИ для распространения вредоносных программ;

попытка проведения кибератаки на веб-приложения и иные сетевые протоколы и службы;

использование вычислительных мощностей объектов ИИ для проведения кибератак.

1.5. Степень критичности инцидента ИБ оценивает начальник ЦИТ или его уполномоченный заместитель по результатам оценки рисков.

2. Уголовная ответственность за преступления в сфере ИБ.

2.1. Правоохранительные или судебные органы могут квалифицировать инцидент ИБ в качестве преступления в сфере ИКТ.

2.2. В уголовном праве Республики Беларусь закреплена ответственность за ряд преступлений против ИБ (Глава 31 Уголовного Кодекса Республики Беларусь – Преступления против компьютерной безопасности):

Статья 349. Несанкционированный доступ к компьютерной информации.

Наказание: штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, арест, ограничение или лишение свободы на срок до 2 лет. Если действия, предусмотренные статьей, повлекли тяжкие последствия – возможно ограничение свободы на срок до 5 лет или лишением свободы на срок до 7 лет.

Статья 350. Уничтожение, блокирование или модификация компьютерной информации.

Наказание: штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, арест, ограничение свободы на срок до 5 лет, лишение свободы на срок до 10 лет.

Статья 352. Неправомерное завладение компьютерной информацией. Наказывается штрафом, лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до 5 лет, или лишением свободы на срок до 7 лет.

Статья 354. Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств. Наказание: штраф, арест, ограничение свободы на срок до 5 лет (с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения), лишение свободы до 10 лет (с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения).

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети.

Наказание: штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, исправительные работы на срок до 2 лет, ограничение свободы на срок до 5 лет, лишение свободы на срок до 7 лет (с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения).

3. План реагирования на инцидент ИБ

3.1. Реагирование на инцидент ИБ включает в себя технические мероприятия, обеспечивающие целостность значимых данных и, при необходимости, возможность судебного исследования этих данных в будущем, а также организационные мероприятия, которые позволяют снизить ущерб от инцидента и составить необходимые для правоохранительных органов документы.

3.2. К техническим мероприятиям относятся:

3.2.1. установка на персональных компьютерах (далее – ПК) каждого рабочего места Университета антивирусной защиты, которая использует: антивирусные сканнеры, мониторы, поведенческие блокираторы, ревизоры

изменений и прочие средства защиты и контроля возможных путей проникновения вирусов на компьютер пользователя, включая Интернет, электронную почту и мобильные носители;

3.2.2. обязательная автоматическая проверка сторонних мобильных носителей информации (USB Flash накопители, жесткие диски и т.д.) на предмет вредоносного ПО на каждом рабочем месте, а также в дисплейных классах, с помощью AVP Kaspersky, ESET либо иной антивирусной программы;

3.2.3. использование различных механизмов шифрования (криптографии) для обеспечения авторства, и исключения возможности внесения искажений в документ (файл с данными);

3.2.4. осуществление контроля входа в ИИ. При использовании ПК, устройство требует от пользователя ввести персональную информацию (имя пользователя и пароль). Доступ к ИИ разрешается только после верификации введённых комбинаций символов;

3.2.5. установка межсетевого экрана, который позволяет снизить число эффективных внешних атак на сеть, несанкционированный доступ к сети организации со стороны рабочих станций, удаленных и передающих серверов, включенных в сеть Интернет, снизить вероятность сбора и мониторинга сетевой информации в интересах третьих лиц, блокировать доступ вредоносной информации в систему;

3.2.6. использование VPN (англ. virtual private network – «виртуальная частная сеть») технологии, алгоритмов криптографирования (электронной подписи, сжатия с паролем, шифрования), что позволяет снизить потери от несанкционированного программно-аппаратного доступа к информации, находящейся в канале связи Интернет, также доступа к информации, размещенной на удаленных и передающих серверах Интернет, сбор и мониторинг информации в интересах третьих лиц;

3.2.7. использование систем ограничения доступа работников и обучающихся к сетевым ресурсам Интернет, использование маршрутизаторов и надежных поставщиков сетевых услуг, кратковременного канала связи, что позволяет сократить сбор и мониторинг сетевой информации в интересах третьих лиц, поток вредоносной информации в систему;

3.2.8. осуществление контроля за соблюдением пользователями и техническим персоналом центра информационных технологий (далее – ЦИТ) правил работы и эксплуатации технических средств в части обеспечения ИБ;

3.2.9. своевременное выявление и оценка причин, условий и характера угроз ИБ, а также дальнейшее прогнозирование развития событий на основе мониторинга инцидентов ИБ;

3.2.10. планирование, реализация и контроль эффективности использования мер и средств защиты информации, создание механизма оперативного реагирования на угрозы ИБ;

3.2.11. резервное копирование изменений конфигурационных файлов технических и программно-аппаратных средств, в том числе средств защиты

информации, восстановление этих файлов из резервных копий, а также хранение соответствующей информации не менее одного года.

3.3. В случае возникновения инцидента ИБ необходимо:

работнику университета сообщить о возникновении инцидента ИБ своему непосредственному руководителю и техническим специалистам ЦИТ, в зоне ответственности которых находится объект, на котором произошел инцидент, и начальнику ЦИТ или его уполномоченному заместителю для принятия необходимых мер по устранению последствий инцидента ИБ и восстановления режима работы;

обучающемуся сообщить о возникновении инцидента ИБ непосредственно преподавателю в аудитории;

специалистам ЦИТ, произвести анализ причин инцидента ИБ и выработать меры для предотвращения подобных инцидентов ИБ в будущем (приобретение или установка необходимого программного обеспечения и (или) оборудования, инструктаж и обучение работников и обучающихся);

всеми вовлеченными сторонами реализовать разработанный комплекс мер для недопущения повторения инцидента ИБ;

при установлении факта обнаружения инцидента ИБ начальником ЦИТ или его заместителем, ответственному специалисту (должностному лицу) необходимо составить докладную записку на имя ректора по установленным фактам нарушения политики безопасности, проведения по ним служебных разбирательств с принятием необходимых мер реагирования;

при выявлении КВУ начальнику ЦИТ либо лицу его заменяющему в течение одного часа оповестить Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты, используя интерактивную форму интернет-ресурса https://cert.by/ с представлением сведений о результатах реагирования и ликвидации последствий инцидента ИБ. Решение об участии национальной команды реагирования в ликвидации последствий КВУ принимается руководителем Национального центра обеспечения кибербезопасности и реагирования на киберинциденты по согласованию с начальником Оперативно-аналитического центра (далее – ОАЦ) при Президенте Республики Беларусь или его уполномоченным заместителем;

при выявлении КВУ, в исключительных случаях начальником ОАЦ или его уполномоченным заместителем принимается решение об участии национальной команды реагирования в ликвидации данного инцидента.

Начальник ЦИТ А.Н.Купо

Проректор по безопасности,
режиму и кадрам
А.М.Куксо
23.05.2024