МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Политика информационной безопасности учреждения образования Университет**

Студент:

Селицкий Данил Евгеньевич

Вариант 11

Преподаватель:

Копыток Дарья Владимировна

Минск 2020

**Содержание**

[Обоснование актуальности, цели и задачи разработки политики информационной безопасности в организации 3](#_Toc63804035)

[Объекты защиты 5](#_Toc63804036)

[Основные угрозы и их источники 8](#_Toc63804037)

[Оценка угроз, рисков и уязвимостей 11](#_Toc63804038)

[Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов 15](#_Toc63804039)

[Вывод 20](#_Toc63804040)

Обоснование актуальности, цели и задачи разработки политики информационной безопасности в организации

В современном Университете хранится и обрабатывается огромное количество различных данных, связанных не только с обеспечением учебного процесса, но и с научно-исследовательскими и проектно-конструкторскими разработками, персональные данные студентов и сотрудников, служебная, коммерческая и иная конфиденциальная информация.

Информация существует в различных формах: на бумажном носителе, в электронном виде при хранении на носителе, передается по почте или с использованием электронных устройств, передается устно в процессе общения. Информация должна быть защищена независимо от ее формы и способа ее распространения, передачи и хранения.

Рост количества преступлений в сфере высоких технологий диктует свои требования к защите ресурсов вычислительных сетей учебных заведений и ставит задачу построения собственной интегрированной системы безопасности. Ее решение предполагает наличие нормативно-правовой базы, формирование концепции безопасности, разработку мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации (СЗИ) в рамках образовательного учреждения. Эти составляющие определяют единую политику обеспечения безопасности информации в вузе.

Специфика защиты информации в образовательной системе заключается в том, что Университет – публичное заведение с непостоянной аудиторией, а также место повышенной активности «начинающих киберпреступников».

Политика Университета в области информационной безопасности предусматривает принятие необходимых мер в целях защиты ресурсов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Университете.

Главные цели Университета не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник Университета. На лиц, работающих в Университете по договорам гражданско-правового характера, в том числе прикомандированных, положения настоящей Политики распространяются в случае, если это обусловлено в таком договоре.

Целью Политики является создание условий, позволяющих предотвратить или минимизировать ущерб, который может быть нанесен в результате несанкционированного доступа, хищения служебной информации или нанесения ущерба техническим средствам обработки, хранения и передачи защищаемой информации.

Под защитой информационных ресурсов следует понимать:

* сохранение конфиденциальности информационных ресурсов;
* обеспечение непрерывности доступа к информационным ресурсам Университета в сферах его деятельности;
* защита целостности служебной информации с целью поддержания возможности Университета по оказанию услуг высокого качества и принятию эффективных управленческих решений;
* повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Университета;
* определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в Университете.

Руководители структурных подразделений Университета должны обеспечить регулярный контроль за соблюдением положений настоящей политики, организовать периодические проверки соблюдения информационной безопасности с последующим представлением ежегодного отчета по результатам указанной проверки руководству.

Объекты защиты

Университет в соответствии с порядком, установленным действующим законодательством РБ, выполняет следующие функции:

1. Определяет перечень специализаций и специальностей, а также направлений научных исследований по профилю университета во взаимодействии с заинтересованными ведомствами и министерствами, организациями и предприятиями на основе изучения потребностей народного хозяйства в специалистах.
2. Разрабатывает и реализует целевые программы в области высшего образования, науки и техники в соответствии со своими профилем совместно с заинтересованными ведомствами и министерствами, организациями и предприятиями.
3. Проводит инновационную политику в области технологий обучения, направленную на эффективную реализацию целей высшего, послевузовского профессионального и соответствующего дополнительного образования, развитие творческой активности научно-педагогических работников и студентов.

Ниже представлены расшифровки аббревиатур типовых подразделений высшего учебного заведения:

* УМУ - Учебно-методическое управление;
* КМО УМО - Координационно-методический отдел УМО;
* УПК - Управление приемной комиссии;
* УРф - Управление по работе с филиалами;
* УМД - Управление международной деятельности;
* УРП - Управление по работе с персоналом;
* УИ - Управление по информатизации;
* ЦСИКНУ - Центр сохранения историко-культурного наследия университета;
* УРГОСО - Управление по работе с государственными органами и связям с общественностью;
* ЦГП - Центр гуманитарной подготовки;
* УО НИР - Управление организации НИР;
* ЦРМП - Центр развития молодежного предпринимательства;
* УПНК - Управление подготовки научных кадров;
* ОРДС - Отдел по работе с диссертационными советами;
* УСВР - Управление по социальной и воспитательной работе;
* ЦРК - Центр развития карьеры;
* УНЦППКРВШ - Учебно-научный центр по переподготовке и повышению квалификации работников высшей школы;
* ПАУ - Прогнозно-аналитическое управление;
* УОЗ - Управление организации закупок;
* УКС - Управление капитального строительства;
* УРСР - Управление ремонтно-строительных работ;
* УЭ - Управление эксплуатации;
* УХС - Управление хозяйственной службы;
* УБ - Управление безопасности;
* ОРУ - Операционно-расчетное управление;
* УСУО - Управление сводного учета и отчетности;
* ОПУ - организационно-правовое управление;
* УКА - управление контроллинга и аудита.

Организационная структура Университета представлена на рисунке 1.

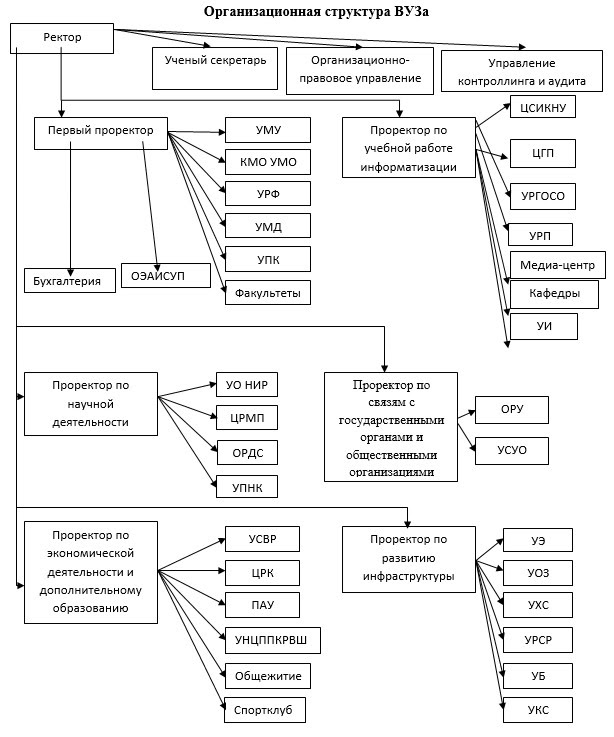


Рисунок 1 — Организационная структура Университета

На основе анализа деятельности подразделений Университета, а также самого университета в целом, составлен перечень типов информации, наиболее нуждающейся в защите:

* персональные данные студентов и сотрудников (отдел кадров, бухгалтерия, факультеты, кафедры);
* информация об информационных технологиях, корпоративной сети, вычислительной сети, программном обеспечении, разработках в области информационных технологий, информационной системе университета (управление по информатизации);
* бизнес-идеи студентов и сотрудников;
* сведения о техническом обслуживании объектов и инженерных сетей (управление эксплуатации);
* политика безопасности, результаты конфиденциальных совещаний (управление по безопасности).

Подлежащая защите информация хранится как в электронном, так и в бумажном виде на серверах университета, на персональных компьютерах сотрудников отделов и в архиве документов; с информацией работают сотрудники указанных отделов, и, соответственно, только сотрудники отделов имеют доступ к соответствующей информации.

Основные угрозы и их источники

Следующим этапом после определения информации, подлежащей защите, является разработка модели злоумышленника.

Модель злоумышленника - абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

Модель злоумышленника включает в себя 4 основных пункта:

1. Цель злоумышленника;
2. Портрет злоумышленника;
3. Направления атаки;
4. Инструменты атаки.

Модель злоумышленника разрабатывается исходя из 4 видов угроз информации:

1. Блокирование.

При блокировании целью злоумышленника является создание условий для отсутствия или ограничения доступа пользователей информационной системы для последующего получения как материальной, так и нематериальной выгоды.

2.Копирование.

При копировании целью злоумышленника является нарушение конфиденциальности информации для последующего оглашения, использования в личных целях или продажи заинтересованным лицам.

3.Модификация.

При модификации целью злоумышленника является изменение информации в системе для причинения ущерба, получения выгоды либо иных личных интересов.

4.Уничтожение.

При уничтожении целью злоумышленника является невозможность восстановления информации ее владельцем для причинения материального и нематериального ущерба.

Для полного описания модели злоумышленника необходимо определить категорию нарушителя: внутренний или внешний злоумышленник.

Внутренним злоумышленником может быть лицо из следующих категорий сотрудников Университета:

* сотрудники факультетов и кафедр;
* сотрудники отдела кадров;
* сотрудники Управления информатизации;
* сотрудники Управления безопасности;
* руководители различных уровней;
* студенты.

Категории лиц, которые могут быть внешними нарушителями:

* уволенные сотрудники;
* технический персонал, обслуживающий здания (уборщицы, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположена информация);
* посетители (приглашенные представители организаций, представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.);
* члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;
* лица, умышленно проникшие в сети университета из внешних (по отношению к ней) сетей телекоммуникации (хакеры).

Сотрудники Управления информатизации и Управления безопасности имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связаны с нарушением действующих правил и инструкций. Особую опасность эта группа нарушителей представляет при взаимодействии с криминальными структурами или спецслужбами.

Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные знания и опыт выделяют их среди других источников внешних угроз.

Конкуренты и криминальные структуры представляют наиболее агрессивный источник внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников университета всеми доступными им силами и средствами.

Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в университете. Наибольшую угрозу представляют криминальные структуры и уволенные сотрудники при взаимодействии с ныне работающими.

Внешние информационные посредники (организации, занимающиеся разработкой, поставкой и ремонтом оборудования, информационных систем) представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам. Конкуренты, криминальные структуры и спецслужбы могут использовать эти организации для временного устройства на работу своих членов с целью доступа к защищаемой информации.

Из вышесказанного следует, что при разработке политики информационной безопасности учреждения, в том числе и Униврситета, необходимо учитывать модель злоумышленника. Чем адекватнее будет модель, тем более полно будет организована защита конфиденциальных данных. Таким образом, построение модели злоумышленника является существенным звеном в организации политики безопасности информационной безопасности на предприятии.

Оценка угроз, рисков и уязвимостей

Виды возможных внутренних и внешних угроз безопасности информации Университета:

* попытки несанкционированного администрирования баз данных;
* исследование сетей, несанкционированный запуск программ по аудиту сетей;
* удаление информации, в том числе библиотек;
* запуск игровых программ;
* установка вирусных программ и троянских коней;
* сканирование сетей, в том числе других организаций, через Интернет;
* несанкционированная откачка из Интернета нелицензионного софта и установка его на рабочие станции;
* попытки проникновения в системы бухгалтерского учета;
* поиск «дыр» в OC, firewall, Proxy-серверах;
* попытки несанкционированного удаленного администрирования ОС;
* сканирование портов и т. п.

Источниками возможных угроз информации являются:

* компьютеризированные учебные аудитории, в которых проходит учебный процесс;
* Интернет;
* рабочие станции неквалифицированных в сфере информационной безопасности работников вуза.

Анализ информационных рисков можно разделить на следующие этапы:

* классификация объектов, подлежащих защите, по важности;
* определение привлекательности объектов защиты для взломщиков;
* определение возможных угроз и вероятных каналов доступа на объекты;
* оценка существующих мер безопасности;
* определение уязвимостей в обороне и способов их ликвидации;
* составление ранжированного списка угроз;
* оценка ущерба от несанкционированного доступа, атак в отказе обслуживании, сбоев в работе оборудования.

Основные объекты, нуждающиеся в защите от несанкционированного доступа:

* бухгалтерские ЛВС (локальная вычислительная сеть), данные планово-финансового отдела, а также статистические и архивные данные;
* серверы баз данных;
* консоль управления учетными записями;
* www/ftp-серверы;
* ЛВС и серверы исследовательских проектов.

Условная численная шкала для оценки ущерба университету от несанкционированного доступа представлена в таблице 1

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб университету |
| 1 | Ущерб от атаки есть, но он незначителен |
| 2 | Ущерб от атаки значителен, но не создаёт угрозы для университета |
| 3 | Ущерб значителен, есть угроза закрытия университета |
| 4 | Университет прекращает своё существование |

Таблица 1 — Условная численная шкала для оценки ущерба университету от НСД

Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам представлена в таблице 2

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

Таблица 2 — Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

Таблица рисков представлена ниже (на основе таблиц 1 и 2)

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риски |
| Спам | 0 | 0,4 | 0 |
| Копирование жесткого диска | 2 | 0,1 | 0,2 |
| Попытки несанкционированного администрирования баз данных | 2 | 0,1 | 0,2 |
| Установка игровых программ | 0 | 0,5 | 0 |
| Установка вирусных программ и троянских коней | 2 | 0,3 | 0,6 |
| Несанкционированная откачка из Интернета нелицензионного софта и установка его на рабочие станции | 1 | 0,4 | 0,4 |
| Попытки проникновения в системы бухгалтерского учета | 2 | 0,1 | 0,2 |
| Поиск «дыр» в OC, firewall, Proxy-серверах | 1 | 0,3 | 0,3 |
| Попытки несанкционированного удаленного администрирования ОС | 2 | 0,2 | 0,4 |

Таблица 3 — Таблица рисков для объектов информационной системы университета

Таким образом можно сделать вывод, что наиболее опасными видами атаки являются установка вирусных программ и троянских коней, несанкционированная откачка из Интернета нелицензионного софта и установка его на рабочие станции и попытки несанкционированного удаленного администрирования ОС, а наиболее частыми атаками являются спам и установка игровых программ.

Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов

В отношении всех собственных информационных ресурсов университета, используемых для получения доступа к инфраструктуре Университета, должна быть определена ответственность соответствующего сотрудника Университета.

Информация о смене владельцев информационных ресурсов, их распределении, изменениях в конфигурации и использовании за пределами Университета должна доводиться до сведения руководителя управления информатизации.

В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим.

В процессе своей работы сотрудники обязаны постоянно использовать режим «Чистого стола (экранной заставки)» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 15 минут.

Каждый сотрудник обязан немедленно уведомить руководителя УИ обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

Доступ третьих лиц к информационным системам Университета должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам Университета должен быть четко определен, контролируем и защищен.

Право удаленного доступа к информационным ресурсам Университета может быть предоставлено только сотрудникам территориально удаленных структурных подразделений и не имеющих прямых физических телекоммуникационных каналов связи компьютерной сети университета и исключительно со стационарных компьютеров, принадлежащих Университету.

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения.

Пользователи портативных компьютеров, содержащих служебную информацию Университета, обязаны обеспечить их хранение в физически защищенных помещениях, запираемых ящиках рабочего стола, шкафах или обеспечить их защиту с помощью аналогичного по степени эффективности защитного устройства, в случаях, когда данный компьютер не используется.

Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности, как в офисе, так и по месту проживания. В ситуациях, когда возрастает степень риска кражи портативных компьютеров, например, в гостиницах, аэропортах, в офисах деловых партнеров и т.д., пользователи обязаны ни при каких обстоятельств не оставлять их без присмотра.

При записи какой-либо информации на носитель для передачи его контрагентам или партнерам по бизнесу необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

Карманные персональные компьютеры, а также мобильные телефоны, имеющие функцию электронной почты, и прочие переносные устройства не относятся к числу устройств, имеющих надежные механизмы защиты данных. В подобном устройстве не рекомендуется хранить конфиденциальную информацию.

Подключение портативных компьютеров к корпоративной сети Университета допускается в исключительных случаях и с ведома начальника.

Все программное обеспечение, установленное на предоставленном Университетом компьютерном оборудовании, является собственностью Университета и должно использоваться исключительно в производственных целях.

Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено неразрешенное к установке программное обеспечение, оно должно быть удалено, а сообщение о нарушении должно быть направлено непосредственному руководителю сотрудника.

На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

* персональный межсетевой экран;
* антивирусное программное обеспечение;

Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной руководителем. Сотрудники Университета не должны:

* блокировать антивирусное программное обеспечение;
* устанавливать другое антивирусное программное обеспечение;
* изменять настройки и конфигурацию антивирусного программного обеспечения.

Электронные сообщения (удаленные или не удаленные) могут быть доступны или получены государственными органами, иными организациями для их использования в качестве доказательств в процессе судебного разбирательства, финансовых или договорных обязательств. Поэтому содержание электронных сообщений должно строго соответствовать корпоративным стандартам в области деловой этики.

Использование электронной почты в личных целях допускается в случаях, когда получение/отправка сообщения не мешает работе других пользователей и не препятствует деятельности Университета.

Сотрудникам запрещается направлять партнерам конфиденциальную информацию Университета по электронной почте без использования систем шифрования. Секретная информация Университета, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

Сотрудникам Университета запрещается использовать публичные почтовые ящики электронной почты для осуществления какого-либо из видов корпоративной деятельности.

Сотрудники Университет для обмена документами с бизнес партнерами должны использовать только свой официальный адрес корпоративной электронной почты.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать специалистов.

Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

Ко всем исходящим сообщениям, направляемым внешним пользователям, пользователь может добавлять уведомление о конфиденциальности.

Вложения, отправляемые вместе с сообщениями, следует использовать с должной осторожностью. Во вложениях всегда должна указываться дата их подготовки, и они должны оформляться в соответствии с установленными в Университете процедурами документооборота.

Пересылка значительных объемов данных в одном сообщении может отрицательно повлиять на общий уровень доступности сетевой инфраструктуры Компании для других пользователей. Объем вложений не должен превышать 10 Мбайт.

Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

В случае кражи переносного компьютера следует незамедлительно сообщить об инциденте начальнику.

Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, согласованны с руководителем управления информатизации.

Вывод

Требования настоящей Политики могут развиваться другим внутренними нормативными документами организации, которые дополняют и уточняют ее.

В случае изменения действующего законодательства и иных нормативных актов, а также устава организации настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также уставу организации. В этом случае ответственное подразделение обязано незамедлительно инициировать внесение соответствующих изменений.

Общий контроль состояния информационной безопасности Учреждения осуществляется ректором. Текущий контроль соблюдения настоящей Политики осуществляет отдел информатизации и связи спутникового мониторинга транспорта.

Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности Учреждения, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий. Отдел информатизации и связи спутникового мониторинга транспорта ежегодно пересматривает положения настоящей политики.

Изменения и дополнения вносятся по инициативе отдела информатизации и связи спутникового мониторинга транспорта или Директора и утверждаются Директором. Порядок пересмотра документов второго и третьего уровней определяется в данных документах.

Все изменения, внесённые в настоящую Политику информационной безопасности должны учитываться в листе «История изменений».